EXHIBIT 25

CoinDesk

Opinion

The 10 Biggest Developments in Bitcoin in 2022

Whether it's the Taro upgrade or growth in the Lightning Network, Bitcoin has seen steady progress this year, says Cory Klippsten, Tomer Strolight and Sam Callahan of Swan Bitcoin.

(Andriy Onufriyenko/Getty Images)

By Cory Klippsten, Tomer Strolight, Sam Callahan

Dec 19, 2022 at 9:41 a.m. PST Updated Dec 20, 2022 at 10:45 a.m. PST CONSENSUS MAGAZINE

Cory Klippsten

Cory Klippsten is CEO of Swan Bitcoin.

Follow @coryklippsten on Twitter

Tomer Strolight

Tomer Strolight is the Editor in Chief at Swan Bitcoin. He began his career as a Bitcoin writer in February of 2021 with the Why Bitcoin Series.

Sam Callahan

Sam Callahan is the Lead Analyst at Swan Bitcoin. He writes the "Running the Numbers" section in the monthly Swan Private Insight Report and the newsletter "The Daily Bitcoiner." He has made multiple appearances on popular podcasts like The Investor's Podcast and the Stephan Livera Podcast.

Price crashes and crypto collapses dominated headlines in 2022, but it was a year of significant progress for Bitcoin. In 2022, we saw how Bitcoin as a protocol allows for widespread innovation that fills whatever needs developers and entrepreneurs identify without any need for changes to that protocol. We've highlighted 10 important developments below.

1. Another year of 100% uptime

The greatest achievement in Bitcoin this year was, once again, Bitcoin itself. Bitcoin continued to operate flawlessly, with one block coming roughly every 10 minutes and its coin issuance precisely adhering to what was set out in Satoshi Nakamoto's white paper in 2008. There were no emergency restarts, no hard forks, no chain splits and no protocol-level hacks or bugs. Yet again, Bitcoin delivered 100% uptime and was available to anyone in the world all year in the face of everything 2022 threw at it. Billions of dollars worth of Bitcoin were transferred every single day on its blockchain.

Bitcoin did all this without any foundation supporting it, without any direct employees, without any leaders or venture capitalists. As such, ongoing developments that rely on Bitcoin's reliability and predictability were able to proceed with uninterrupted focus for yet another year and with the confidence that they'll be able to do so for the foreseeable future.

It is worth noting that none of the remaining items on this list require any changes to Bitcoin's base layer consensus rules.

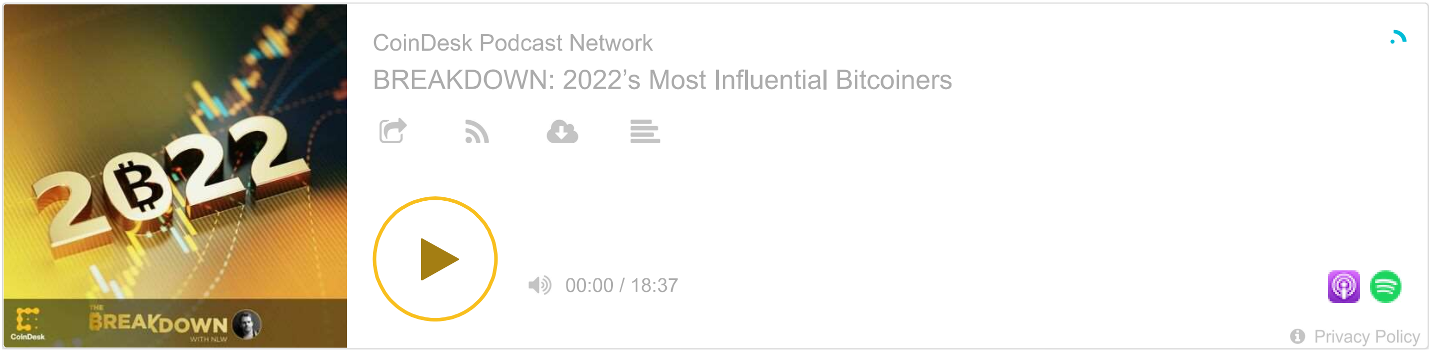
2. Growth of the Lightning Network

While Bitcoin's base layer remains rock steady, its most significant scaling protocol, the Lightning Network, experienced massive growth and development in 2022. Lightning Network allows for instant, cheap payments off-chain, eliminating the need to wait for a block to confirm transactions. It is entirely decentralized and permissionless and improves Bitcoin's scalability while still leveraging the security and settlement assurances of Bitcoin's base layer. The network's publicly visible liquidity capacity rose from 1,058 BTC to more than 4,771 BTC in 2022.

The number of Lightning Network channels rose by +80%, from 37,298 to 67,339 channels.

The number of publicly visible Lightning Network nodes increased by +88%, from 8,295 to 15,636 nodes (though the rate of growth slowed in the second half).

All told, the growth of the Lightning Network was astounding this year, driven by numerous wallets that were launched, better tools for users that were built, and more educational resources that were produced. Instant, cheap payments (typically under 1 U.S. cent) became widespread in 2022 as Bitcoiners looked to exchange value peer-to-peer over the Lightning Network.



3. El Salvador – where no nation has gone before

In 2022, El Salvador experienced the greatest country rebrand in history under President Nayib Bukele's policy of economic liberty and Bitcoin. Bukele appeared on the cover of Bitcoin Magazine's year-end edition, which showed the president looking like the Founding Father of hyperbitcoinization, the first mover and the leader who dared to embrace Bitcoin-only and the economic liberty it offered to his people.

Read more: What Is Bitcoin's Lightning Network?

In the column, Bukele called for all Bitcoiners around the world to recognize that El Salvador's fight against the global elites is their fight, too. El Salvador's embracement of the bitcoin currency made clear to all that it understands exactly what revolutionary money actually is, despite the FUD from mainstream media. While U.S. regulators and political elites got taken in by the likes of Sam Bankman-Fried, bitcoin led to boom times in El Salvador. Tourism numbers have skyrocketed, GDP is growing and the country keeps stacking sats.

October saw the creation by El Salvador of the world's first “Bitcoin Embassy” in Lugano. This chamber of commerce will be headed by Salvadoran bitcoin miner and investor turned Bitcoin diplomat and “Honorary Consul” Josue Lopez. November saw the creation of the Bitcoin Office within the Office of the El Salvadoran President. The office was created to meet the growing demand for access and information from investors worldwide. The Bitcoin Office further establishes the El Salvador template for more nations to copy on the road to hyperbitcoinization. El Salvador closed out the year in the most bitcoin way of all – with President Bukele announcing that El Salvador would start buying one bitcoin every single day.

You have received 10.5K sats 0.00010502 BTC is worth around 34 Z from lighteing:

You have received 5K sats (0.00005000 BTC is

(Machankura)

4. Machankura – transacting with bitcoin over text in Africa

This new service was coded in a few weeks by African developer, Kgothatso Ngako, who noticed a problem – most Africans have basic phones but don't have access to a reliable internet connection – so he created a solution. Machankura enables people in Africa to receive and spend bitcoin via text messages without needing an internet connection. In a report from Caribou, 94% of financial transactions in Africa are made through text messages, and only 6% of these transactions are made via mobile apps. This new service allows individuals throughout Africa to use bitcoin for the first time on technology that is already at their disposal. Projects like Machankura will help push bitcoin adoption in regions that need digital sound money the most.

5. Taro – assets on the Lightning Network

This year, Lightning Labs introduced a protocol proposal to Bitcoin and the Lightning Network that aims to allow for the minting, sending and receiving of assets on the networks. Taro utilizes Bitcoin's latest protocol upgrade, Taproot, to enable the issuance of theoretically any kind of asset on the Bitcoin blockchain while still using the immutable verification of Bitcoin's proof-of-work consensus mechanism. Taro could allow for all kinds of assets like stablecoins, stocks, and bonds to be issued on top of the Bitcoin protocol opening the door for more use cases and more functionality on the network.

6. Impervious.ai – The first P2P Lightning-native browser

Impervious Technologies launched the first web browser built on top of Bitcoin's second-layer scaling system, the Lightning Network. It is a peer-to-peer web browser that offers a full suite of tools for communication, data transfers,and Lightning payments without any middlemen. This comes in the form of secure peer-to-peer messaging, P2P video calls, P2P workspaces, decentralized identity management, decentralized data storage and direct user monetization of their data. All of these tools are fully encrypted, and they remove centralized intermediaries that collect and sell the user's data. By utilizing the decentralized nature of the Bitcoin and Lightning networks, Impervious Technologies has given us a hint of what the Internet will look like in the future.

7. FediMints – collaborative custody

FediMint is a new method to custody bitcoin by forming collaborative custody communities to help secure each others' bitcoin and protect privacy. This form of custody takes advantage of the inherent fact that humans trust those closest to them the most. It leverages technologies like federations and (David) Chaumian e-cash mints to cryptographically maintain privacy between the individuals of a group while also allowing them to share custody of the entire group's bitcoin. This custody solution offers the possibility to scale bitcoin, improve privacy, lower on-chain fees and can get more individuals to take self-custody of their bitcoin around the world.

8. Value-4-Value – embedding payment functionality anywhere

Value-4-Value is a new approach to content publishing where the creator receives value after the "customer" enjoys the content, once again, through the Lightning Network. Over 10,000 content creators have already implemented Value-4-Value on their podcasts, and solutions such as LightningAddresses and Bolt-12 invoices, are making this possible for all other types of content, promising continued rapid growth in 2023.

9. Plebnet Lightning – community tools to make Lightning more functional

An informal Telegram group of ordinary people interested in running their own Lightning nodes formed and is about to cross over 5,800 members.

Not only do participants provide support to each other on best practices, but community members have developed and released numerous open-source applications to make some of the most advanced capabilities of Lightning Network easily accessible to anyone. sdLightning Terminal is a browser-based interface for managing channel liquidity on self-hosted Lightning nodes, performing submarine swaps via the Lightning Loop service, classifying channels and integrating loopd, poold, and faraday daemon. Balance of satoshis makes it easy to balance channels, making it easy to issue lightning transactions that balance channels' inbound and outbound liquidity. LNDg and Lightning Jet offer similar capabilities with more advanced features for monitoring nodes and maximizing efficiency.

10. Gridless computing with BTC mining

All over the world, people live with very little, very expensive or no electricity. Bitcoin mining is changing all this. One example, shared by Twitter founder Jack Dorsey, was powering a rural Kenyan village while securing the Bitcoin network with excess hydropower, all while lowering rates to 2,000 people (500 families) by approximately $10 a month to only $4.

Far from being an isolated example, a further $2 million in the financing, led by Stillmark VC and Block, was secured in December to use bitcoin mining to increase energy access across Africa while further distributing and securing the Bitcoin network.

CoinDesk.tv
I'LL TAKE BITCOIN FOR $500, ALEX
BUY BITCOIN
CANADA
CoinDesk.tv
MYTH-BUSTING BITCOIN MISCONCEPTIONS

Read more about

Opinion Bitcoin Lightning

Issue 17

Most Influential 2022

Explore This Issue

More from Consensus Magazine

Consensus Magazine

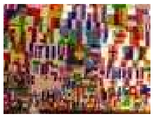
After FTX: How Congress Is Gearing Up to Regulate Crypto

Jesse Hamilton Jan 23, 2023

Consensus Magazine

The World's Best Crypto Policies: How They Do It in 37 Nations

Jeff Wilser Jan 23, 2023



Consensus Magazine

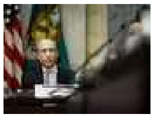
The Bizarre (Sort of) Bipartisanship of the Crypto Congress

Jeff Wilser Jan 25, 2023

Consensus Magazine

What If Regulators Wrote Rules for Crypto?

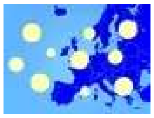
Michael Selig Jan 23, 2023



Consensus Magazine

MiCA at the Door: How European Crypto Firms Are Getting Ready for Sweeping Legislation

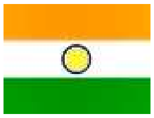
Anna Baydakova Jan 24, 2023



Consensus Magazine

India Has Clamped Down on Crypto. What Will It Do With Its G-20 Power?

Amitoj Singh Jan 24, 2023



Consensus Magazine

'We Haven't Seen Anything Yet': Introducing CoinDesk's 'Policy Week'

Ben Schiller Jan 23, 2023

Consensus Magazine

'What Was Gary Gensler Really Doing?': Rep. Tom Emmer on FTX, the SEC and What's Next for Crypto in Congress

Jeff Wilser Jan 23, 2023

BTC	$24,541.47	▲ 1.93%	→
ETH	$1,681.61	▲ 0.91%	→
BNB	$313.55	▼ 0.30%	→

XRP	$0.39392919	▼ 1.19%	→
APT	$15.35	▼ 3.43%	→

View All Prices

Sign up for First Mover, our daily newsletter putting the latest moves in crypto markets in context.

Email address

Sign Up

By signing up, you will receive emails about CoinDesk product updates, events and marketing and you agree to our terms of services and privacy policy.

DISCLOSURE

Please note that our privacy policy, terms of use, cookies, and do not sell my personal information has been updated.

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups. As part of their compensation, certain CoinDesk employees, including editorial employees, may receive exposure to DCG equity in the form of stock appreciation rights, which vest over a multi-year period. CoinDesk journalists are not allowed to purchase stock outright in DCG.

Trending

1 Policy

Compute North's Reorganization Plan Approved by Bankruptcy Judge

Feb 16, 2023

2 Policy

CFTC Charges California Firm and CEO With Fraud, Misappropriation of Digital Assets

Feb 16, 2023

3 Policy

Binance Moved Funds From US Affiliate's Silvergate Bank Account in 2021: Reuters

Feb 16, 2023

4 Web3

Blur Surpassed OpenSea in Daily NFT Trading Volume Wednesday, Nansen Shows

Feb 16, 2023

CoinDesk

About

About
Masthead
Contributors
Careers
Company News

Stay Updated

Consensus
Newsletters
Follow

Get In Touch

Contact Us
Advertise
Accessibility Help
Sitemap

The Fine Print

Ethics Policy
Privacy
Terms Of Use
Do Not Sell My Personal Information

Please note that our privacy policy, terms of use, cookies, and do not sell my personal information has been updated.

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups. As part of their compensation, certain CoinDesk employees, including editorial employees, may receive exposure to DCG equity in the form of stock appreciation rights, which vest over a multi-year period. CoinDesk journalists are not allowed to purchase stock outright in DCG.

English ▾

CoinShares

15TH DEC 2022 • 50 MIN READ • MATTHEW KIMMELL

Taro: A New Asset Issuance Protocol on Bitcoin

LAYER 1 SMART CONTRACTS PAYMENTS

Key Takeaways

- Taro draws on the new features introduced by the 2021 Taproot soft-fork to enable new types of asset issuance and spending on the Bitcoin and Lightning Networks.

- While Taro's associated risks are not yet fully understood by the Bitcoin community, nor has its full abilities been properly tested in practice, its specification outlines exciting opportunities to evolve the Bitcoin network to settle more forms of asset exchange, such as those involving tokenised fiat currencies (stablecoins), tokenised securities, or non-fungible tokens (NFTs).

- The risks, such as technical complexity and third-party dependencies, stem from structural challenges of enabling more flexibility into Bitcoin, its reliance on newly activated Taproot features, and the unavoidable necessity of externally sourcing price and/or issuance data for stablecoins, securities and NFTs.

- If successful, Taro has the potential to advance financial inclusion, greatly increase the usefulness and network effect of the Bitcoin Network, improve Bitcoin's resistance against censorship attacks, and foster greater payment privacy.

- At CoinShares Research, we find the possibility of stablecoins being enabled on Bitcoin's Lightning Network is a particularly promising development capable of disrupting both traditional and crypto native payment rails; however, it is still unclear to us whether Taro will be an effective way to accomplish this, and exactly how these developments will progress beyond their conceptual stages.

- In the event Taro succeeds at onboarding new users to the Lightning network, it could be a major catalyst in spreading the idea of bitcoin to new groups of adopters who may not yet have explored its potential and properties as money. This could help bitcoin win an increasing share of the global monetary market, adding incremental value to each bitcoin unit in line with our fundamental investment thesis.

Introduction

In this post, we explore the broader possibilities and implications of a new Bitcoin Improvement Proposal, Taro, which introduces a framework for custom asset creation inside of the Bitcoin Monetary System. Taro is structured to ensure that it remains fully voluntary for network participants and does not increase the resource requirements (storage, bandwidth, etc.) of node operators—in other words, it does not negatively impact the decentralisation of the Bitcoin Network.

At the same time, Taro enables new kinds of assets to be compatible on Bitcoin's second-layer Lightning network for those who wish to use it. This provides several key differences to previous attempts at issuing assets atop Bitcoin, with which we'll cover later in this piece.

Other than increased complexity, there are no significant downsides to the proposal, and its most controversial aspect is likely to be the lack of current demand for new types of assets within Bitcoin itself.

Those most enthusiastic seem to envisage Taro expanding the potential of Bitcoin's Lightning network to a more general purpose payments system, capable of transferring numerous assets beyond bitcoin. We find Taro likely most appealing to those that view Bitcoin as a settlement system, and believe its layered architecture is an optimal engineering design to both deliver the full suite of services required to complement and/or rival modern financial services and at the same time avoid introducing vulnerabilities to the system's core—a provision we'll cover in more detail later.

We conclude that while many will be encouraged by the potential of Taro, it has yet to be properly tested, and patience will be important for any anticipated improvements to meet their expectations and challenge existing alternatives while also not compromising the unrivalled security and stability of the Bitcoin Network.

For the curious reader unfamiliar with Lightning, we suggest first reading our explainer here, which summarises and offers context as to how Lightning adds an added layer of abilities to Bitcoin. It may also be helpful to read our primer of Taproot, the latest major software change to Bitcoin, on which Taro directly relies.

This series however will skip over those discussions, and focus on the history leading up to Taro (Section 4), its general structure (Section 5), the potential new features it may present users, and the effects they may have on Lightning and the broader Bitcoin ecosystem (Section 6 & 7).

In particular, we explain the possible impact of introducing fiat currencies on Lightning and the opportunities Taro may bring for Bitcoin developers more generally. We also examine some of the challenges associated with Taro and other considerations we find are necessary for it to realise its potential.

Background

Before delving into the details of Taro, it will probably be interesting for readers to understand some of the history behind the issuance, hosting and transfer of new kinds of assets within the Bitcoin ecosystem. Bitcoin was created to enable individuals to transact digital value directly with each other, and without relying on any third party. And as promised, users can effectively hold, send, or receive bitcoin without the added *necessary* friction of financial institutions and intermediaries (commercial banks, payment processors, etc), without counterparty risk, and with decentralised settlement.

While the Bitcoin protocol is suitable to perform the fundamental monetary functions of bitcoin, its base layer doesn't offer the flexibility to natively issue other types of assets or perform more elaborate financial transactions that are commonplace in the real world economy. This is a conscious design choice made to keep Bitcoin as simple and free of attack vectors as possible—the fewer moving parts, the fewer fundamental problems are likely to arise.

Commonly traded goods (such as fiat currencies, equities, debt, collectibles, etc) can already utilise bitcoin as a unit of account, and Bitcoin as a settlement system, but they are not natively recognised within the Bitcoin monetary settlement system itself. In other words, these items can be priced in bitcoin and economically represented through transactions recorded on the Bitcoin blockchain, yet the items themselves, and their prices, must be represented elsewhere.

This is similarly (and perhaps counterintuitively) also the case in the modern financial system. Here, goods are often measured in dollars and exchanged through intermediaries like brokerages or payment processors, only to be finally reconciled and economically represented through simple dollar transfers on primary settlement systems (like FedWire, or CHIPS).

With this, the traditional system enables investors to access financial markets to manage their capital in more complex ways, and do so in a scalable manner; however, in turn, it also requires trust in the specially privileged organisations and private networks on which the primary settlement systems depend (often, large bulge bracket banking institutions).

The concept of Bitcoin evolving to settle value more akin to the modern financial system has thus stimulated a vigorous debate around how to best replicate real world assets and financial services without sacrificing the robust, trust minimised, and decentralised properties Bitcoin offers.

A somewhat common stance is that some of the layers of the financial system will eventually be rebuilt or doctored to stack atop Bitcoin as a primary settlement system. This system is already settling significant amounts of value every year, recording $4.7 trillion in 2021 and is currently on pace to settle $4.2 trillion in 2022.

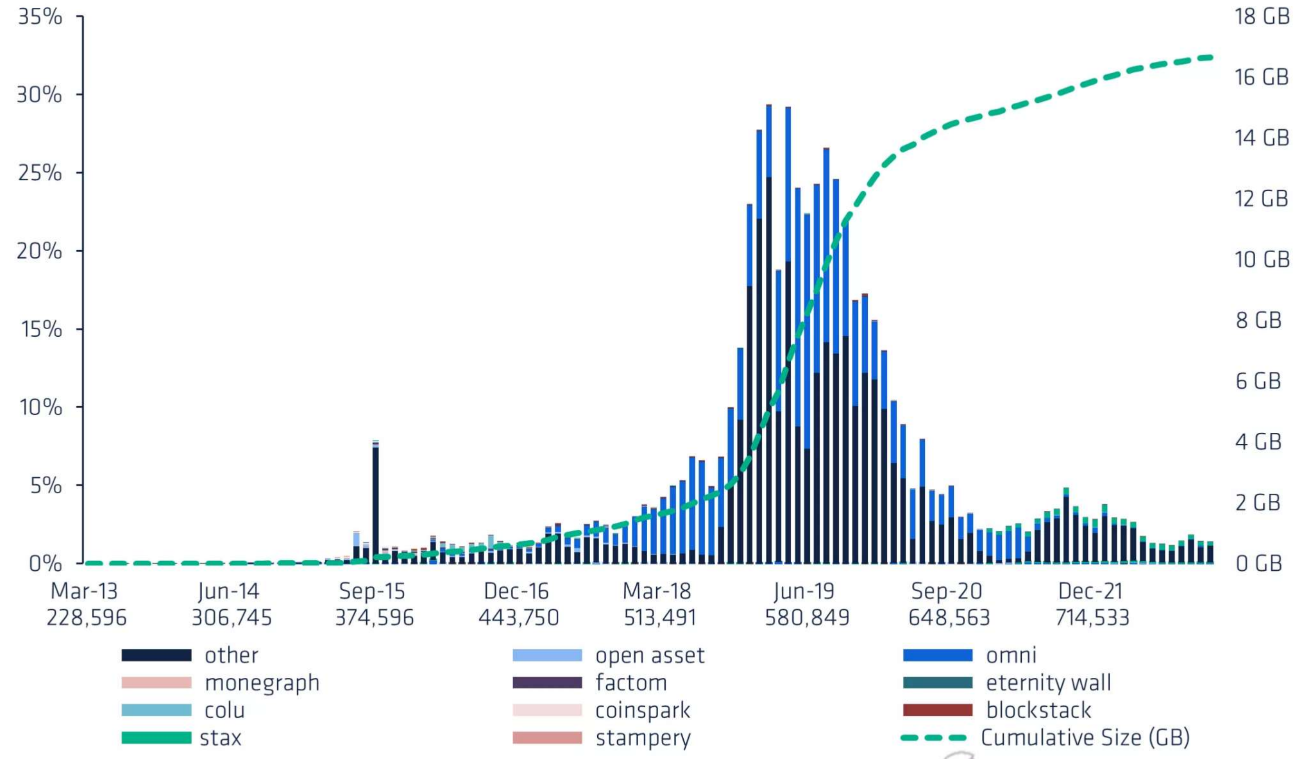
We caution that this is not necessarily a consensus view, but in our opinion, as a result of Bitcoin having a governance system that is both openly accessible and completely voluntary it has amassed a community of broad and oftentimes conflicting perspectives. Without direction by any particular person or group, Bitcoin does not have a conventional roadmap, leaving room for factions and partisan behaviour on how Bitcoin should progress, or ossify. In this way, there is no certainty as to how Bitcoin's ecosystem will change moving forward, if at all.

The historic journey we're about to embark on will show exactly how complicated, prolonged and controversial this can make Bitcoin's evolution. Bitcoin is a system that requires widespread agreement for developments to be accepted, and this agreement can be quite difficult to attain.

The Tried but Not True Method for Creating Customised Bitcoin Assets

Early attempts at distributing new assets on Bitcoin proved to be creative yet unpolished, leading to experimentation that would actually come to lay the groundwork for popular Ethereum applications while at the same time highlighting certain challenges that ultimately stifled adoption within Bitcoin.

Figure 1: OP_Return Percentage of Total Bitcoin Transactions, Monthly



Source: BigQuery, Coinmetrics, opreturn.org, CoinShares, data available as of close 07 December 2022
Op_Return transactions do not include coinbase transactions

CoinShares

These projects essentially created software that would interpret additional transaction data (which can be added to Bitcoin transactions for some extra cost) as the issuance or spending of outside assets. Specifically, this meant publishing standardised messages to a nondescript compartment of a transaction (called OP_return), watching for such transactions on the blockchain, and creating a trail of ownership on a separate record system. Although not welcomed by Bitcoin developers at the time, this technique does not violate any of the Bitcoin rules.

The most prominent of these projects, Counterparty, Colored Coins, and Mastercoin (later rebranded to Omni), reached legitimate milestones when considering the broader cryptocurrency landscape today, launching what is commonly deemed the first Initial Coin Offering (ICO) and Decentralised Exchange (DEX), as well as several other precursor technologies.

These early projects had significant traction, accounting for 24% of transactions in 2019. However, they were not by any stretch of the imagination universally popular within the Bitcoin community. In our view, the mixture of an unwelcoming community, scalability and other technical issues, plus an eventually fast-growing competitive environment outside of Bitcoin limited their success.

We'll attempt to summarise these issues below.

Community Discouragement

Many of the techniques[1] used by token creation projects were highly criticised and even considered parasitic to Bitcoin. The fact that storing data unrelated to transfering bitcoin was involuntary for network members was seen by some as abusing limited network resources, and even evidence of a free-rider problem. The point being that inordinate data recorded to the blockchain would have the undesirable consequence of Bitcoin requiring more storage and memory, raising the hardware requirements for existing network members and increasing the entry cost for new ones, creating certain friction to the spread of entities enforcing Bitcoin's rules.

In other words, it would threaten to reduce the decentralisation of Bitcoin.

Some considered the possibility of widespread issuance of arbitrary assets (of, shall we say, dubious real-world value) on Bitcoin deeply unethical and contrary to the spirit of the protocol and community—many of whom are deeply concerned with *credibly* levelling the financial playing field. The inevitable proliferation of scams and resulting losses to members within the Bitcoin ecosystem was considered to be a major risk to the system's credibility.

Others, on a similar note, opined that these projects were detracting from the community's primary objective of delivering a decentralised and trust minimised monetary network. Adding new assets was perceived as an unnecessary opportunity cost, and the idea that a small group would be given the privilege of managing and controlling the sales and proceeds of issuing assets was considered unfair.

Ultimately, we find the general disapproval among Bitcoin community members was the largest deterrent to the success of these projects, and a main catalyst for both the creation of—and later explosion of tokens issued on—Ethereum, as well as the cultural divide that remains between the two largest cryptocurrency projects.

Usability

The user experience of issuing and spending these tokenised assets was somewhat slow, costly, and often involved dated graphical interfaces. We'll make an example out of Counterparty, one of the most adopted asset issuance projects built on Bitcoin.

Creating a Counterparty asset generally required both downloading their official wallet software as well as paying a fee in XCP, the project-specific token (which at least to its credit could only be created by burning bitcoin, and has since been available for purchase on secondary exchange markets). To then spend such an asset, on say the Counterparty DEX or a betting application, the owner was subject to the bottleneck of Bitcoin's ten minute block interval. Recipients would then either have to run their own Counterparty node, or they would have to trust the Counterparty network operators were acting honestly in tracing the correct trail of Counterparty asset transactions within the Bitcoin blockchain.

The trust assumptions are similar to those of Bitcoin users not running their own node, which is probably not an issue for casual low-value use. The ten minute block time however is probably a larger problem for these types of projects. While a couple hours is a reasonable amount of time to settle large sums of money, any type of stablecoin, financial transaction, or even game would likely be rather hamstrung if all types of transactions needed time on the order of hours to reliably process (hence why layers like Lightning are critical parts of the Bitcoin technology stack).

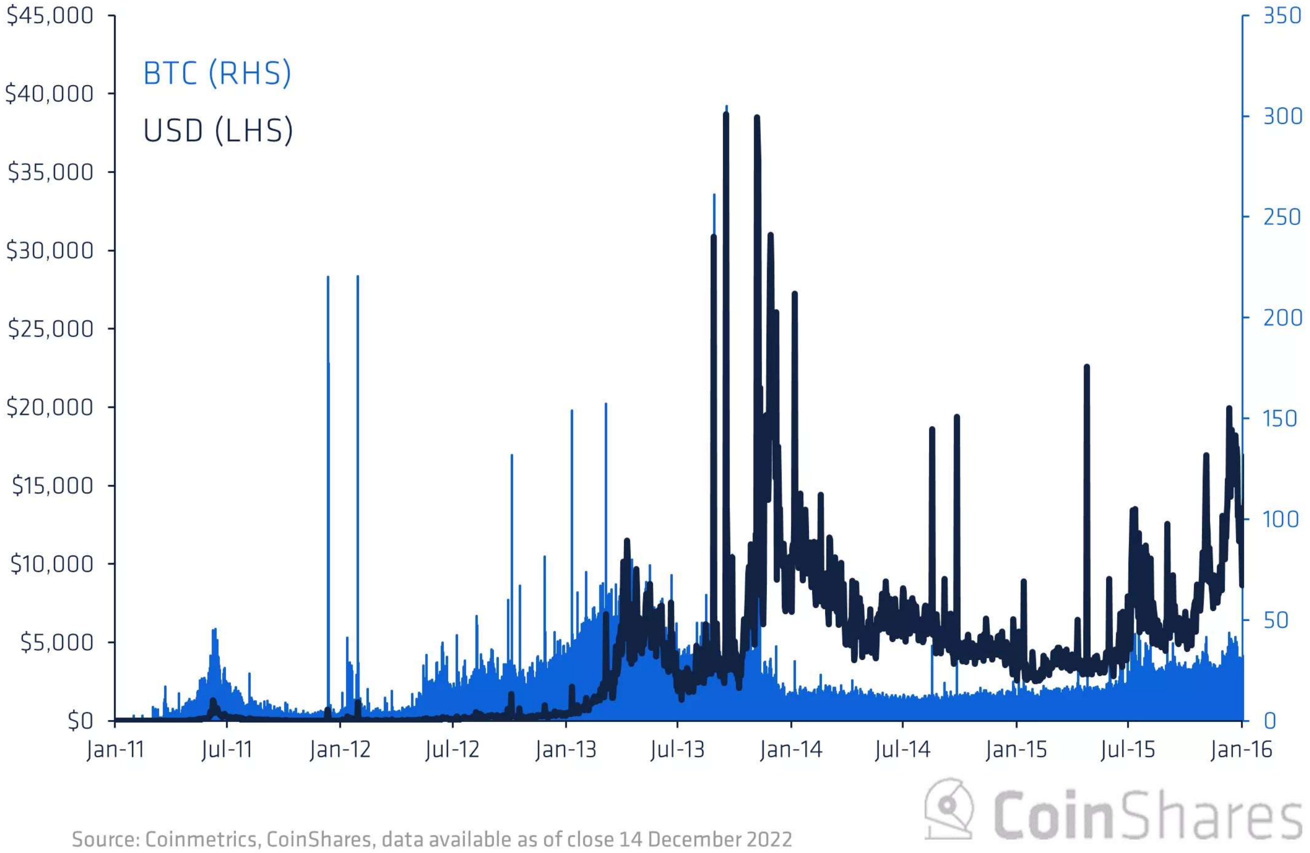
This may exemplify the crux of all Bitcoin-based applications of the sort — any transfer will explicitly be limited by the speed of Bitcoin blocks. This means a simple asset swap would almost certainly require several minutes before materialising on an exchange's order book. However, it doesn't seem like this was a major issue to users at the time, perhaps due to a lack of alternatives or the excitement over promising new functionality.

Scalability/Costliness

Making a bitcoin transaction requires paying an associative fee, and when making transactions of greater data intensity, such as the multisignature and Op_Return ones used by asset creation protocols, the necessary fees are often higher than average.

Bitcoin fees however are also auction-based, so for as long as blocks are not full, they will tend to zero. This was the case for almost 5 years. However, by 2013 bitcoin fees were starting to make themselves felt as an unavoidable aspect of sending a transaction, even though they were lower in dollar terms than they are today.

Figure 2: Total Daily Bitcoin Fees, USD and BTC (2011-2016)



Source: Coinmetrics, CoinShares, data available as of close 14 December 2022

Despite a lack of evidence that this was a significant problem, we suspect it might have become one had these projects gained more traction. It might perhaps have been comparable to the stifling fee environment Ethereum endured throughout the frenzied experimentation of DeFi applications over the past year or so where most casual transactions got crowded out by extremely valuable ones.

The potential of a damagingly high fee environment was not lost on the Bitcoin community, adding further negative sentiment to the idea of these projects in their heyday, and perhaps fueling the arguments of future large blockers in the Blocksize Wars that were to follow in the not-so-distant future.

Fungibility

Some community members have also expressed concerns regarding the fungibility of coins when used as containers for other assets. Representing arbitrary assets using bitcoin could cause some random denominations of bitcoin to dramatically exceed the value of other equal denominations.

Bitcoin outputs that carry alternative assets are also often times more identifiable such that malicious miners can single them out for discrimination. Meaning, miners that determine which transactions are included in a block could censor, or purposely leave out, ones that carried assets beyond bitcoin.

Competitive Environment

The advent of Ethereum in 2015 brought an alternative blockchain that made trade-offs against decentralisation, robustness, attack surface, and trust to offer more complex transaction scripting—essentially enabling code of any complexity to be executed directly within the settlement system. This, along with the design choice of faster block intervals, made application usage much more user friendly compared to Bitcoin.

In addition, Ethereum disrupted the aforementioned projects built on Bitcoin by welcoming and encouraging the general community of proponents that were keen to experiment with new kinds of cryptographic assets. By generally prioritising the usability of developer tools, it has continued to host the most valuable crypto assets outside of bitcoin, as well as be the platform of choice for issuing new assets.

However, it is worth mentioning that Ethereum itself has also lost market share due to competitive forces, best evidenced by Solana and Tron, other cryptocurrency platforms that offer comparable functionality but feature even higher throughput, faster processing, and lower transaction costs, at the further incremental cost of decentralisation and trust minimisation.

In the end, most of these types of projects left the Bitcoin ecosystem while Bitcoin developers tried to figure out how, if at all possible, to enable such uses within the

Bitcoin technology stack. Meanwhile Ethereum blossomed until it, too, inevitably ran into many of the problems predicted by developers in the early days of Bitcoin, in turn spawning a whole industry of ‘expressive blockchain protocols’.

Almost ten years later the pieces may finally have fallen into place within the Bitcoin protocol itself, and in the next part of our series we will explain how it might be done and what consequences it could have.

Taro Enables Asset Issuance on Bitcoin With Fewer Tradeoffs

Taro is best explained as an evolution of the techniques put forth by the early Bitcoin-tethered asset issuance protocols Mastercoin and Counterparty. However, it is an entirely new design, improving upon some of their limitations by drawing upon the new features introduced with Taproot, and thereby reducing the total amount of undesirable tradeoffs. But perhaps most significantly, due to its compatibility with Lightning, Taro might finally have introduced a way to issue and transact new kinds of assets within the Bitcoin ecosystem without running into unsolvable scaling constraints.

The tradeoffs introduced by Mastercoin and Counterparty were covered in more detail in Section 4 of our report on Taro, but we also list them below as a reminder:

- Increasing resource requirements for network operators — Undesirable because it threatens to reduce the decentralisation of Bitcoin

- Reducing transaction fungibility — Undesirable because it makes it easier to discriminate against transactions by nefarious miners

- Limited capacity to scale — Undesirable because it limits the growth potential of servicing new users and increasing usage

- Lacking Privacy — Undesirable because it threatens to reduce the safety of users

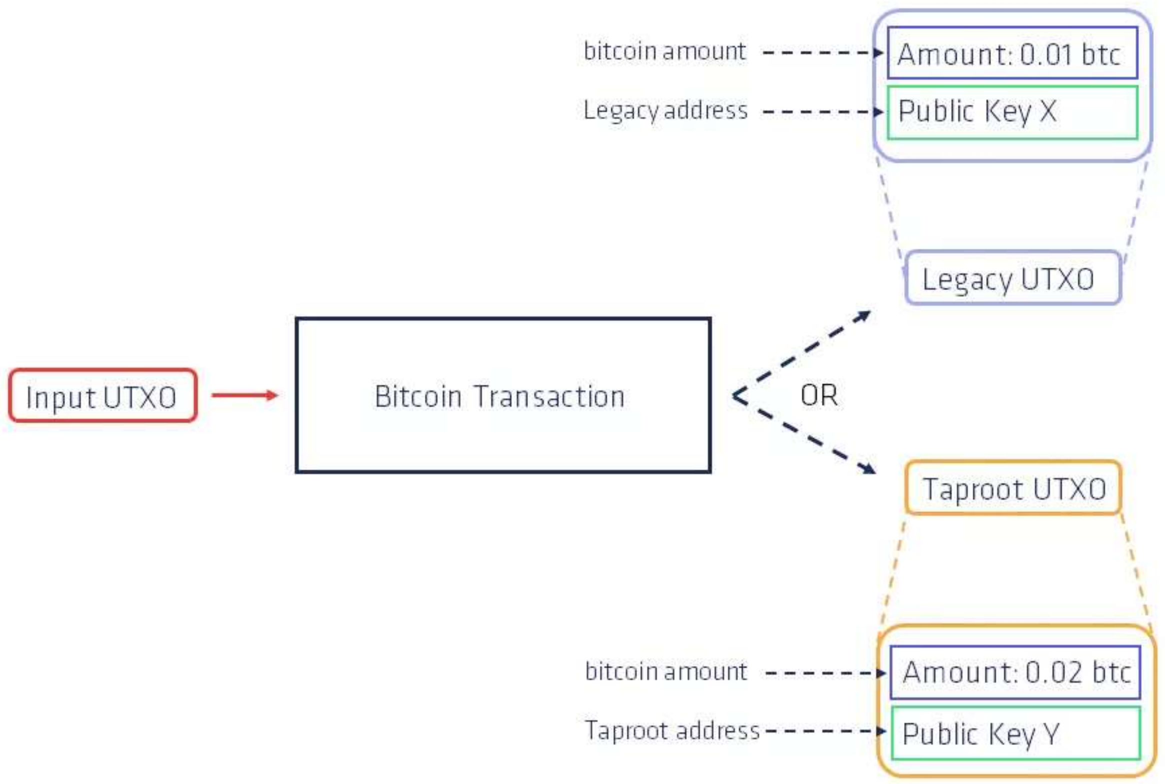
Past protocols have struggled to design systems for issuing custom assets without making at least one of the above trade-offs, leading to significant discouragement from within the Bitcoin community and ultimately, limited adoption. Taro however makes use of recent advancements in the Bitcoin technology stack that did not exist at the time when the aforementioned protocols were launched. Specifically, this includes Bitcoin's most recent major soft fork, Taproot, and the speedy payments protocol, Lightning which itself was introduced following the previous major Segregated Witness (SegWit) soft fork from 2017.

Taro relies on Taproot to improve efficiency and privacy, reduce censorship risk, and enable Lightning integration for quick, cheap and scalable payments

Together, the features of both Taproot and Lightning allowed Lightning Labs — the creators of Taro — to propose a methodology with a broadly similar purpose of issuing and spending assets whose information rides and resides in data fields inside of bitcoin transactions. But this time around, it is being done in a way that offers greater scalability, protects privacy, mitigates censorship risks, and perhaps most importantly, does not increase the resource costs of base network participants.

Before describing how Taro works, we'll first briefly explain some of the properties of Taproot and Lightning that have provided the technical foundation to, at least in theory, sidestep the undesirable trade-offs of previous protocols:

Figure 3: Taproot Enables the Creation of a New Type of Transaction Output (UTXO)



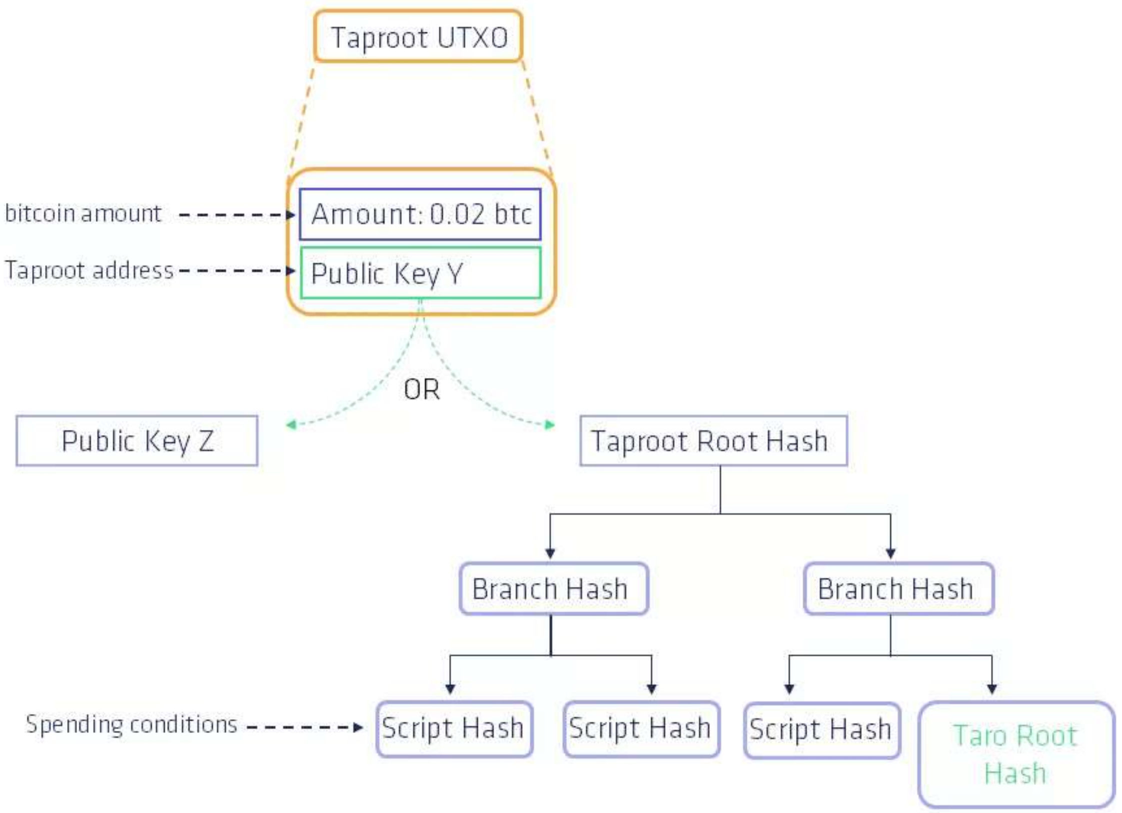
Taproot

- Taproot enables a new way of spending bitcoin (sometimes referred to as a transaction output type, or UTXO) which allows coins to be spent either by the owner of a standard private key, or by anyone who can satisfy a specific set of requirements determined by the transaction creator (often called a smart contract)

- Taproot transaction outputs containing specific spending requirements look indistinguishable to any other Taproot transaction on the Bitcoin blockchain, so no one can determine whether such a transaction is a 'regular' bitcoin transfer or a smart contract until after it has been spent

- Taproot transactions are more resource efficient compared to other bitcoin transaction types that may also be used to spend complex transactions

Figure 4: In Taro UTXOs, the Address can be either a Public Key or a Taproot Root Hash



In the case of Taro, the increased flexibility of Taproot transactions allows for the extra information about outside assets to travel as part of a bitcoin spend (more on how this works, later). Importantly, due to the privacy properties of Taproot, Taro spends are indistinguishable from other Taproot transactions. This means that miners cannot censor Taro spends, as it is unlikely anyone could identify which Taproot transactions are carrying Taro assets.[2]

Lightning

- The Lightning Network uses the concept of payment channels to increase the economic capacity which can be settled in bitcoin transactions

- The Lightning Network effectively has no limit to its transfer speed (other than the speed of light) or overall capacity, and is extremely cheap compared to other payment networks

- The Lightning Network offers stronger privacy than Bitcoin's base layer since most transaction information is never seen by anyone that is not directly involved in the transaction itself (the tradeoff being that Lightning is less decentralised and trust-minimised)

The ability for Taro assets to retain compatibility with the Lightning Protocol enables them to make use of the same cheap and speedy second layer payments network that native bitcoin currently benefits from. This enables the use of Taro assets to expand outside the scaling constraints that are built into the base layer Bitcoin ecosystem to safeguard its decentralisation. It also enables Taro assets to potentially benefit from applications that are also building compatibility into the Lightning protocol.

Taro Works by Recording Asset Ownership in an Off-Chain Database, Relying on Client-Side Validation, and Maintaining Compatibility with the Lightning Network

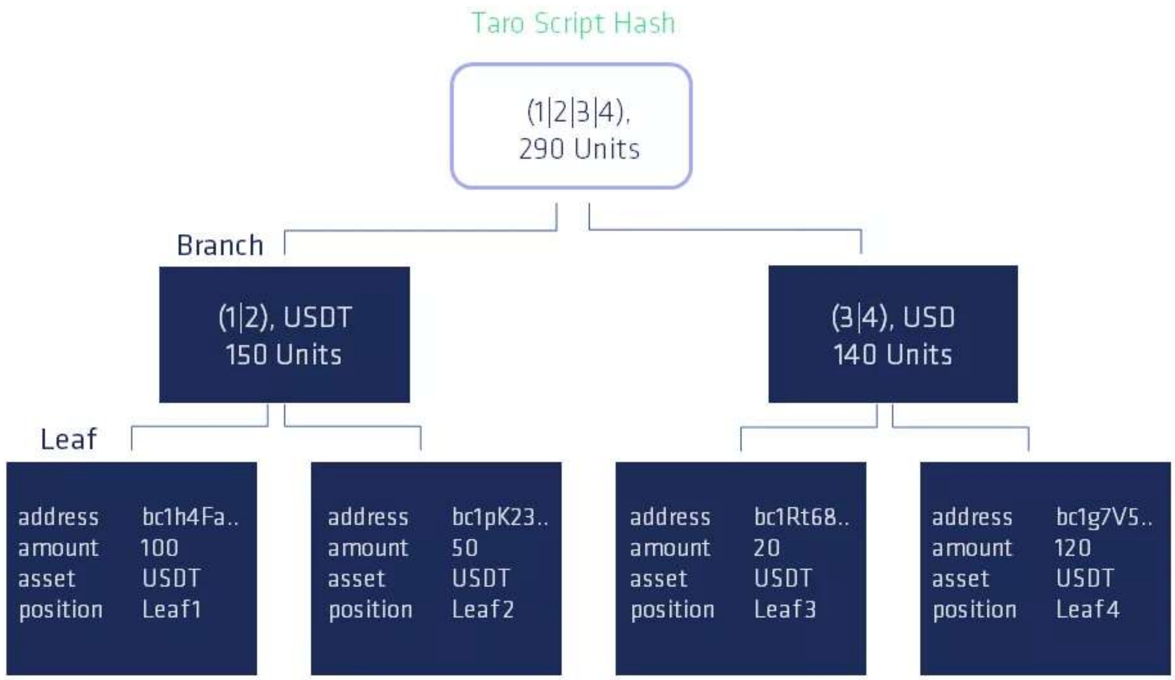
Rather than recording raw asset data in the optional data fields of a conventional transaction, which is both publicly viewable and must be stored by all network members, Taro data is structured and stored off-chain, and only by those that voluntarily opt in. All the necessary proof that is needed for Taro to work is contained in the Taproot address itself, which takes up no more space than any other bech32 address.

In other words, to a non-Taro user, Taro Taproot addresses look like any other address and can be anything, but a Taro user looking at a particular Taproot address will be able to recognise and verify that it contains the information that they need to transact Taro assets.

Recording of Taro Ownership is Done in Distributed Off-Chain Databases

Balances of all Taro asset holdings are logged in standardised off-chain databases that are stored and updated individually by Taro participants. The function of these databases is to prove to each individual Taro user that they indeed own their assets, and enable them to embed the necessary information for further Taro transfers. Each type of asset has its own set of databases and users only need to keep databases for the assets they care about. This directly increases the resource requirements on Taro users, but *not* on any other non-Taro Bitcoin nodes.

Figure 5: The Taro Script Hash Contains a Tree-like Structure of Taro Assets



The Taro Script Hash database is designed as a tree-like structure containing one or more Taro assets. At the bottom, each asset owner, represented by a Taro address, has their own account, or "leaf", with an accompanying balance that denominates the number of assets an owner holds. A "branch" is then a collection of leaves that equate to the sum of several owners, and the "root", which is a sort of checksum of the entire tree contents, represents all owners in the tree. This tree is essentially the building block of Taro, needed to understand how many assets an owner possesses.

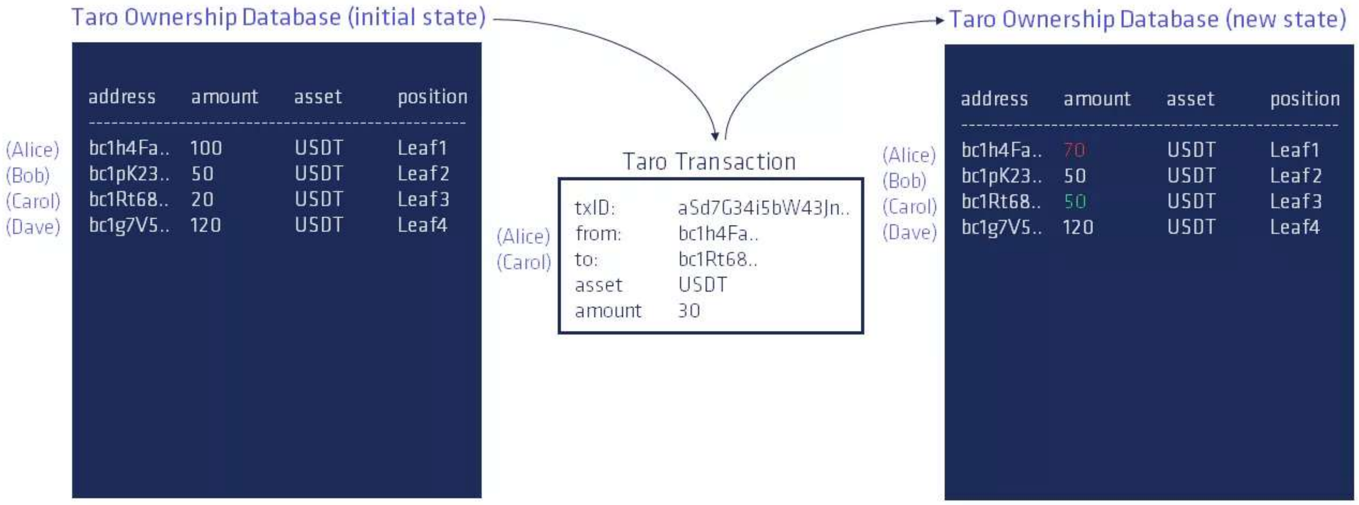
A key aspect of the Taro ownership database is that the checksum or root, which contains a sum of each owner's balance within the tree, is plainly available to each Taro user, such that a recipient is able to quickly verify the total amount of assets in a database. In traditional Bitcoin fashion, this is meant to enable Taro participants to verify that their assets have not been maliciously inflated.

However, no user can see any information concerning any leaf belonging to anyone other than themselves and users with which they have previously transacted. In other words, no individual user has full access to any entire database. Users have access to enough information to verify incoming transfers, but not enough to know the balances or transaction histories of other random users. Only the asset issuer has a somewhat higher level of visibility than other users, but even they start losing visibility once transactions start taking place.

On-Chain Transactions Bind New and Updated Versions of The Distributed Off-Chain Taro Databases to The Bitcoin Blockchain

When a Taro asset is first created or when additional supply is issued, the issuer generates a new ownership tree, assigns a user/balance pair to the appropriate leaves, and attaches it to a bitcoin output. Each subsequent spend of this bitcoin then prompts an updated version of the Taro databases stored by each of the involved sending and receiving parties. It also generates a new Taproot address which contains cryptographic proof (a checksum of sorts) that both the changes made to each Taro users' holdings are effective and no additional Taro assets have been created out of thin air, essentially anchoring each change in Taro ownership to specific transactions recorded in the Bitcoin blockchain.

Figure 6: Taro Transactions Alter the Off-Chain Databases of the Involved Users



Taro Ownership Database (initial state)

	address	amount	asset	position
(Alice)	bc1h4Fa..	100	USDT	Leaf1
(Bob)	bc1pK23..	50	USDT	Leaf2
(Carol)	bc1Rt68..	20	USDT	Leaf3
(Dave)	bc1g7V5..	120	USDT	Leaf4

Taro Transaction

	txID:	aSd7G34i5bW43Jn..
(Alice)	from:	bc1h4Fa..
(Carol)	to:	bc1Rt68..
	asset	USDT
	amount	30

Taro Ownership Database (new state)

	address	amount	asset	position
(Alice)	bc1h4Fa..	70	USDT	Leaf1
(Bob)	bc1pK23..	50	USDT	Leaf2
(Carol)	bc1Rt68..	50	USDT	Leaf3
(Dave)	bc1g7V5..	120	USDT	Leaf4

A clever aspect of how Taro leverages Taproot is that this ownership data itself is not actually recorded to the Bitcoin blockchain, nor will it alter the appearance of a transaction to look like anything other than a run-of-the-mill spend. Taro uses the properties of Taproot to embed specific requirements to a bitcoin output that both must be met to spend the bitcoin and are unrecognisable to the common observer. The key requirement in Taro's case, is to produce a new version of the ownership tree that rightly debits the spender and credits the receiver.

Said another way, anyone intending to spend their Taro asset is required to have both the private key associated with the asset *and additional off-chain data* that allows them to prove to their counterparty that they will no longer control the asset after the transaction. Taro thereby creates an off-chain record system of these alternative assets, which can subsequently be transferred using bitcoin transactions.

The Validation of Taro Transfers is done by Senders and Receivers, not Bitcoin Nodes

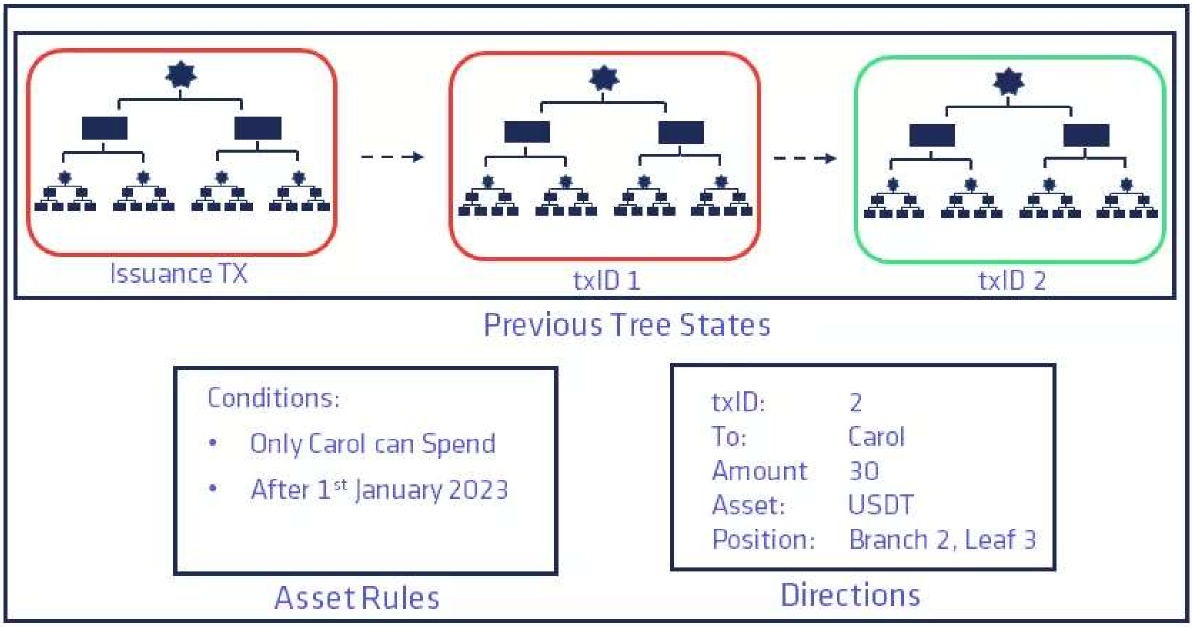
Since the general Bitcoin network is not aware of any Taro asset exchange, and therefore cannot use the general Bitcoin rules to clarify whether a transfer is correct, the sender and receiver are expected to authenticate whether a Taro transfer is valid by themselves. The burden of proof in this process is on the sender, who crafts and communicates a message to the receiver.

A Taro transfer therefore consists of a message from sender to receiver, to authenticate that the sender has the necessary funds, and that after the transaction is spent, the receiver will be in control of these funds.

Importantly, these messages are meant to only be known by the sender and receiver, safeguarding both the privacy of the transactors and also other Taro asset owners. They include several key pieces of information to validate the transfer of funds, such as:

- Which bitcoin transaction originally created the ownership tree
- The issuer of the Taro asset
- All the previous versions of the ownership tree
- Directions to verify the balance of the receiver has been correctly increased, and
- Any specific rules on how to spend the Taro asset

Figure 7: Taro Transaction Proofs Contain Previous States, Asset Rules and Directions

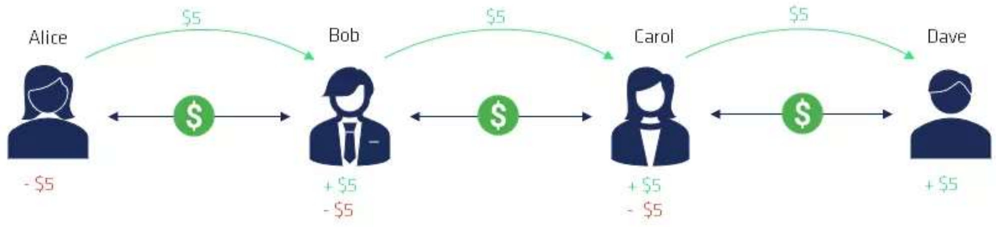


A helpful analog of the Taro transfer process may be to imagine the spender communicating a secret map to the recipient comprised with the information necessary to trace the asset's history, including: the Taproot transaction containing the Taro asset's issuance; the subsequent transactions since then; and, the directions for the recipient to find the exact location of their asset leaf in the most recent Taro ownership tree. It is therefore this map, or "cryptographic proof", that enables the recipient to confirm that the correct account balances have been debited and credited by the spender, and also that the assets transferred were actually issued by the entity they expect.

Taro assets integrate with Lightning, just like bitcoin

Taro in its most basic form is a standardised way to use Taproot's features, however its greatest potential (which we'll discuss further in Section 6 of our Taro report) lies in its compatibility with the Lightning protocol. This means fungible Taro assets can be lifted into payment channels[3] to leverage the benefits of a cheaper, faster, and more scalable payments network.

Figure 8: Lightning Transactions 'Hop' Between Users Connected by Channels



The process of Taro assets being lifted into the Lightning network is similar to that of native bitcoin. A channel opening is a smart contract transaction agreed upon between two parties, the information of which is contained within a Taproot address. Like native bitcoin, Taro assets on Lightning can then be transacted off-chain.

However, upon closing a payment channel infused with Taro assets, the resulting final balance of each partner's Taro holdings is submitted as an update to the Taro ownership database. As far as Bitcoin is aware, this will appear as a standard Taproot transaction, exactly like any other on-chain Taro transfer.

The key difference between bitcoin and Taro on Lightning is that Taro assets will never *actually* be recorded to the Bitcoin blockchain. Otherwise, the process of opening/closing a Lightning channel, as well as sending/receiving Lightning payments, is effectively the same.

Taro is a Supplementary Software that Fits within the BTC/LN Technology Stack

In Section Two of our Taro report, we mentioned that Taro may be most appealing to those that view Bitcoin as a settlement system, and believe its layered architecture is an optimal engineering design to both deliver the full suite of services required to complement and/or rival modern financial services and at the same time avoid introducing vulnerabilities to the system's core. Let's now take a closer look at how Taro may fit into this framework.

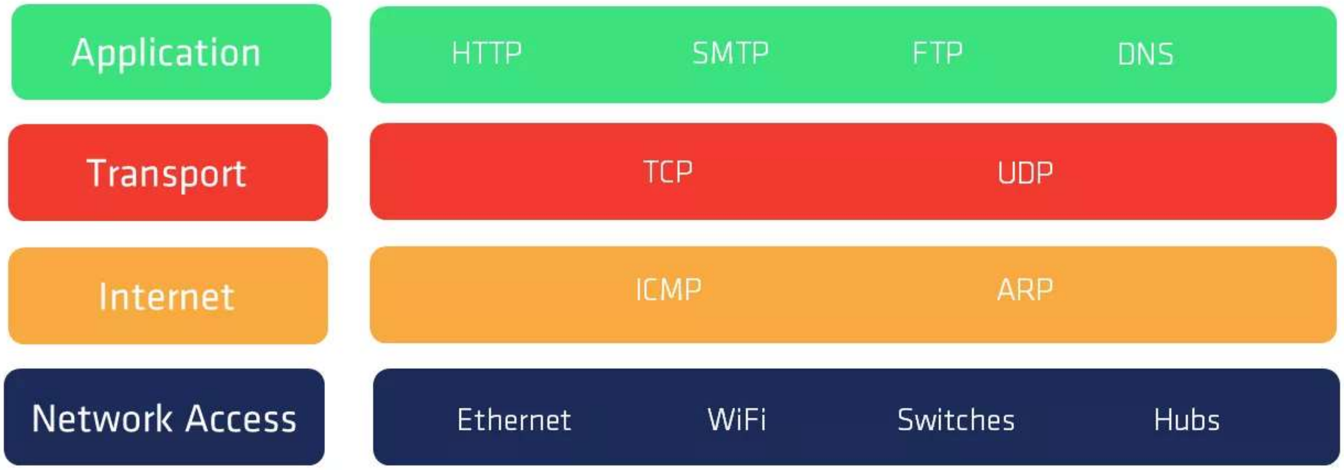
Taro *does not require any changes* in the Bitcoin or Lightning protocol rules. Taro software releases do not magically allow current Bitcoin/Lightning network members to recognise new assets and will not require them to make any changes. Rather, Taro is standalone software with its own rules that can be run alongside the Bitcoin and Lightning protocols, offering those network members a choice to be cognisant of assets beyond bitcoin.

In this sense, Taro works as supplementary software that layers atop the existing Lightning and Bitcoin software stack. To join the Taro network, a node operator must already be a part of the Bitcoin network and abide by the Bitcoin rules.[4] This means that Taro members are part of the Bitcoin system rather than being segregated into an entirely new system. Specifically, they are required to both be part of the Bitcoin network and operate with additional sets of rules and resource requirements. Taro members who then choose to also run Lightning software will be able to both create connections and route payments within the existing Lightning network.

Taro therefore does not make any changes to Bitcoin's core system. It is instead a modular add-on that directly relies on already established components within Bitcoin software. A helpful mental model may be that another layer is being laid on top of the already established foundation that is the Bitcoin protocol.

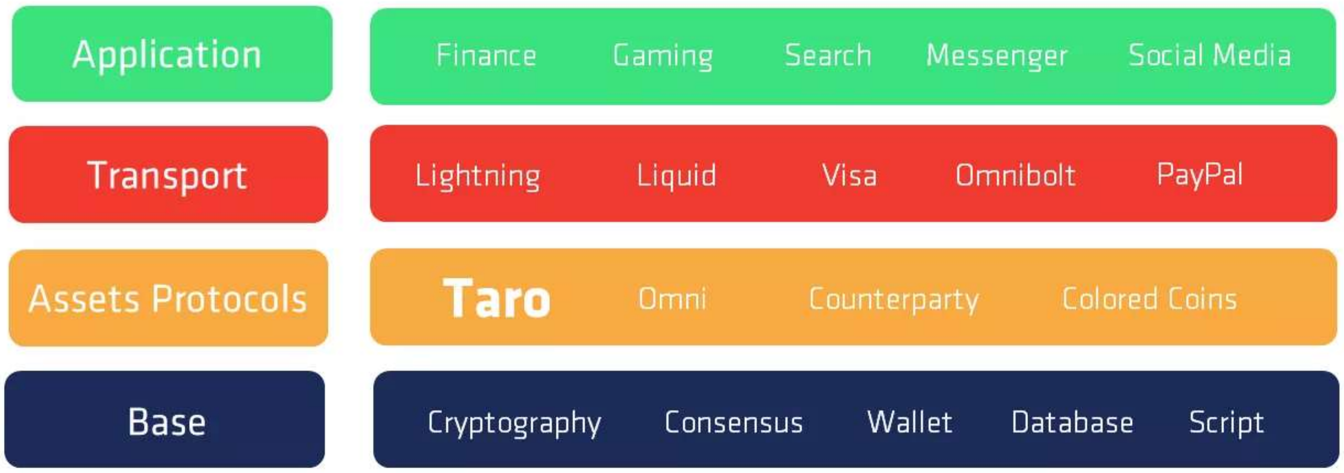
Layered network protocol architecture is not a new concept. For example, the Internet protocol suite evolved into several layers, each with their own specialised purpose: web pages use HTTP, e-mails use SMTP, machine addressing uses IP, and packet routing uses TCP. The analogy of layers is not perfect, but it can help us conceptualise and perhaps better understand the relationships between the components of more complex systems. When it comes to the internet, every interaction touches a variety of protocols across many taxonomic layers, from the base physical wires in the ground to the applications we interface with on a daily basis.

Figure 9: The Internet Network is Structured in Several Layers



Bitcoin is showing signs that it is developing its own form of technology stack, also composed of a suite of protocols each designed for a specialised purpose. Like the Internet, the base layer is completely relied upon by higher layers, and it rarely changes outside of backwards-compatible advancements in efficiency. Higher layers on the other hand tend to see more frequent experimentation, and are more likely to evolve into the entry points with which consumers more commonly interface.

Figure 10: The Bitcoin Network is Structured in Several Layers



Taro seems to be a new layer fitting somewhere in the middle of the emerging Bitcoin technology stack, designed to enable new kinds of assets to be spent on higher layer payment networks and/or utilised in higher level applications — something we plan to cover further in future reports.

Major Taro Opportunities

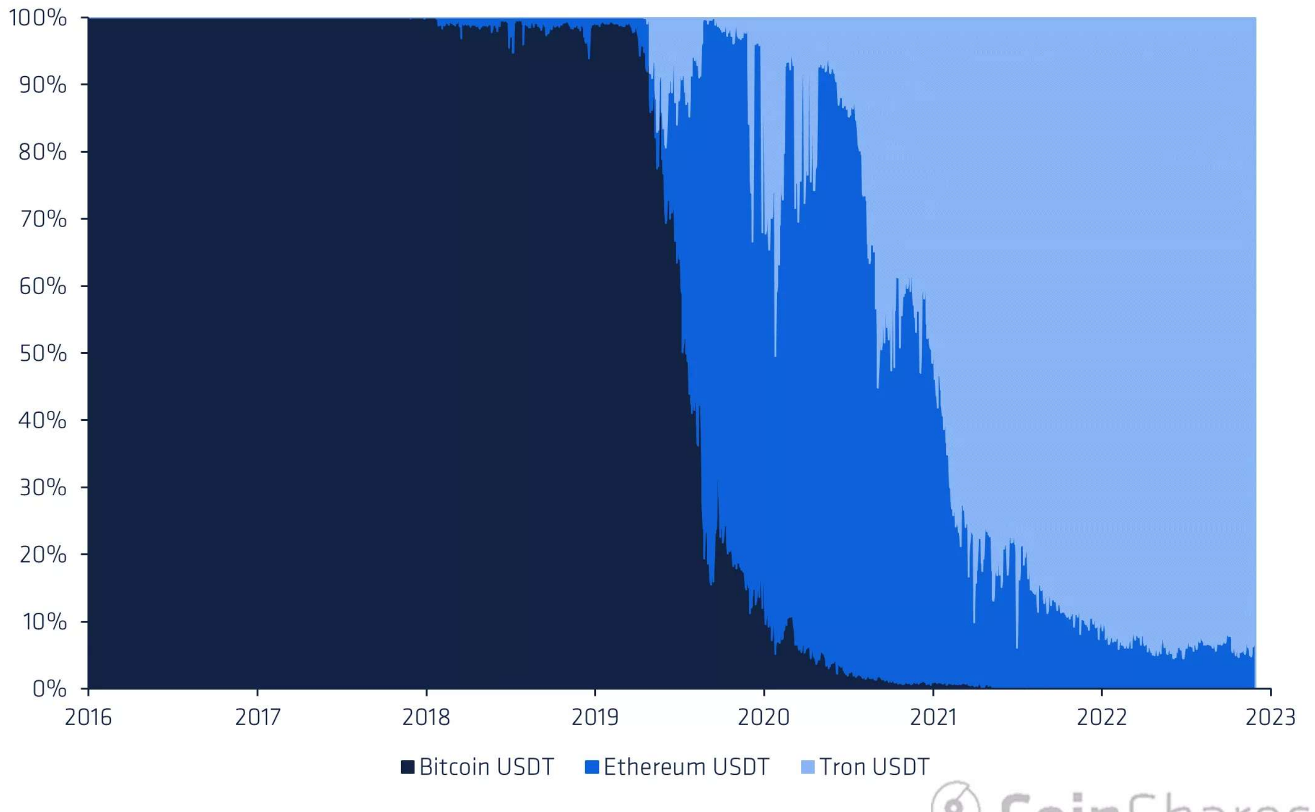
Efficiency

A significant part of the motivation for creating Taro was to enable the transaction of US Dollar stablecoins on the Bitcoin Lightning Network. Crypto representations of the US dollar (dubbed "crypto dollars" or "dollar stablecoins") have dramatically risen and grown in usage to the extent that they are arguably the predominant use case of many generalised blockchains systems (such as Ethereum, Tron, Solana, BNB Chain etc.).

By nature of being 'Layer 1' blockchains, these systems are often exposed to unavoidable transaction fees and/or limitations on transaction throughput. Steadily growing demand and inefficiencies of on-chain architectures have therefore traditionally posed a large and constant opportunity for disruptive innovation and/or new market entrants.

This trend has been observable since the first successful dollar stablecoin Tether began its life on Bitcoin's OMNI protocol (previously Mastercoin, discussed in Section 4), before running into capacity and fee problems. It then migrated to Ethereum until the same exact problems manifested and it moved further out towards more centralised, lower-fee and higher-throughput chains such as Tron, BNB Chain and Solana. This clearly reflects a need among stablecoins for transactions to be as fast and cheap as possible.

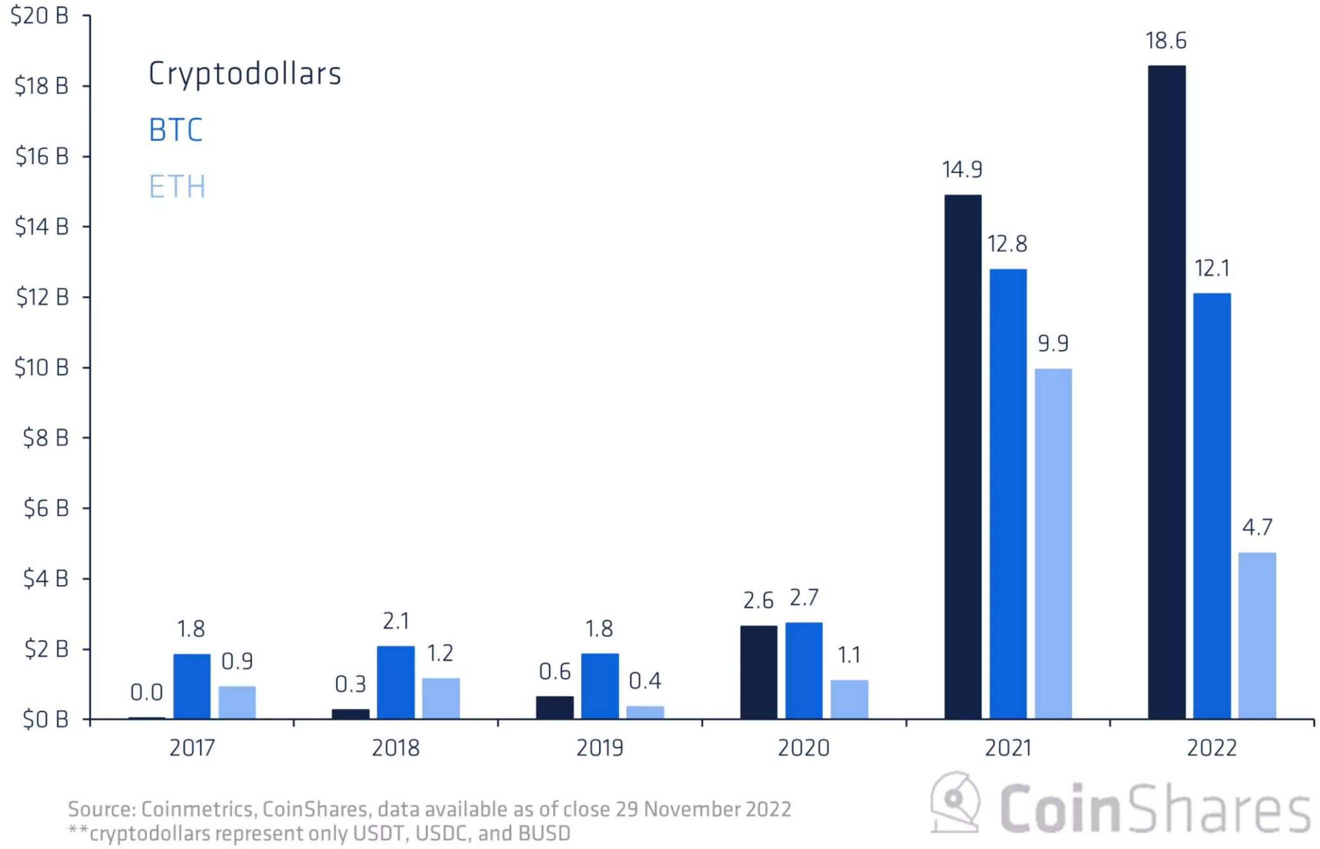
Figure 11: Evolution of Tether (USDT) Transfers on Crypto Platforms



Source: Coinmetrics, CoinShares, data available as of close 28 November 2022

Since 2021, the daily average settlement value of the top crypto dollars has surpassed that of any other cryptocurrency; roughly 38% of centralised exchange volume involves a crypto dollar trading pair; and, three of the top seven cryptocurrencies by market cap (equivalent of $130 billion, at the time of writing) are crypto dollars issued by bank-like crypto firms, namely Binance, Tether, and Circle.

Figure 12: Daily Average Settlement Value by Asset (USD)



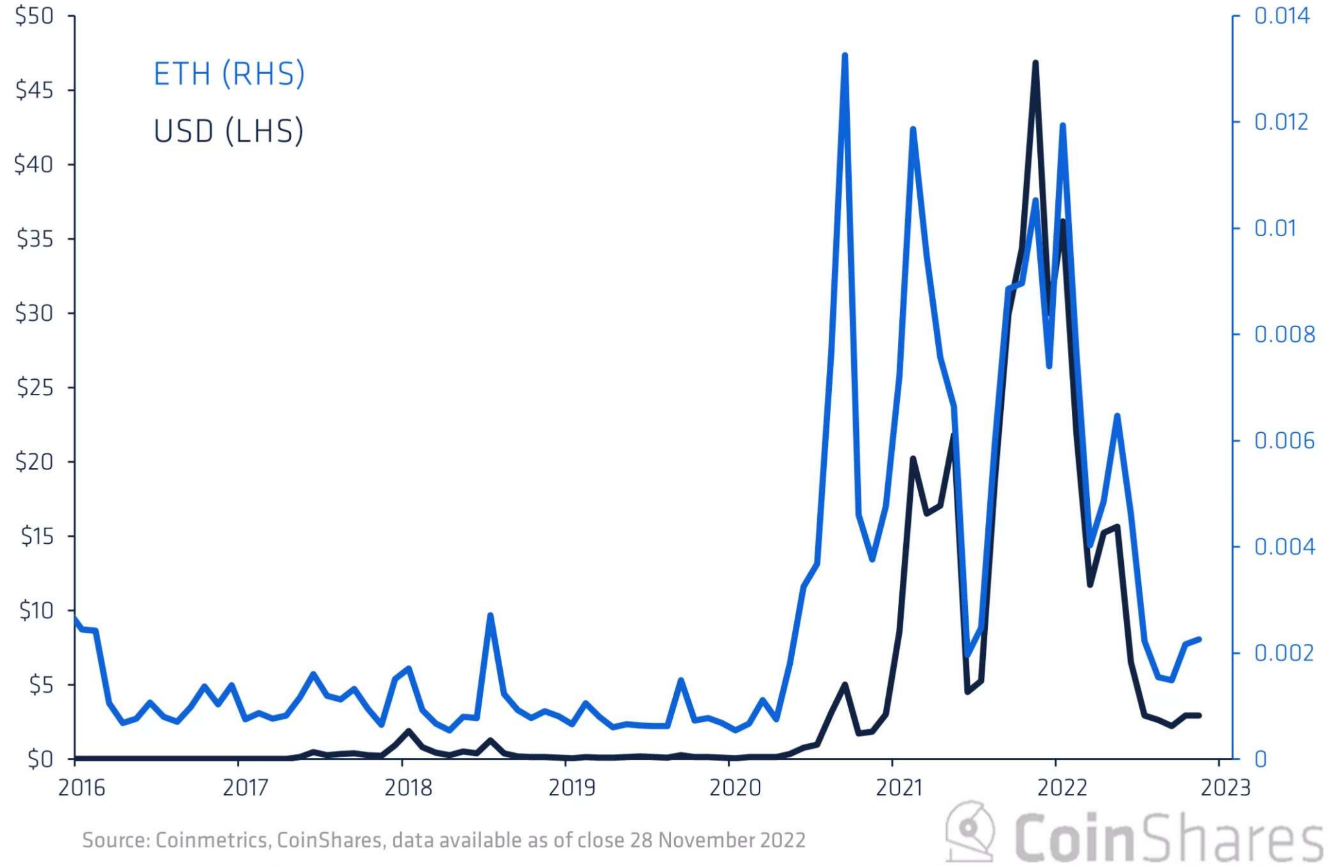
Source: Coinmetrics, CoinShares, data available as of close 29 November 2022
**cryptodollars represent only USDT, USDC, and BUSD

Stablecoins enable traders to gain or retain exposure to US dollars without needing to exit the crypto ecosystem. The tokens ride on crypto rails and are often self-custodial and transferred without the requirement of Know-Your-Customer (KYC) compliance or without needing to involve the banking system. This has made them highly popular among cross-exchange arbitrage traders and among citizens suffering under capital controls or other forms of monetary repression.

However, crypto dollars today almost entirely rest upon blockchain platforms that may be somewhat politically encumbered, poorly structured, centralised and/or unstable due to being pushed to the technical limits of what blockchains can do in terms of throughput. In turn, unsuspecting users have been vulnerable to systemic collapses or access denial, as was the case by certain Terra and Ethereum users this past year.

In parallel, the scalability issues of crypto systems (stemming from all participants storing, verifying, and relaying each valid transaction) has also led to stretches of high payment costs and long transaction waiting times.

Figure 13: Ethereum Average Transaction Fee Levels, Monthly



Source: Coinmetrics, CoinShares, data available as of close 28 November 2022

This presents an opportunity for Taro by offering the option to settle crypto dollar transactions on the blockchain with the longest history, highest stability, least technical debt, and strongest settlement assurances. In our opinion, the crux here is Lightning network compatibility which would enable the cheapest and fastest way to transfer crypto dollars, leading us to suspect that the success of a dollar-pegged

Taro asset would almost certainly cause some level of migration among crypto dollar users back toward the Bitcoin ecosystem.

In a mature state, the Lightning network may evolve into a globally predominant payments platform and we believe the introduction of flexibility in the types of assets that may be transferred is a step in the right direction.

Accessibility

Taro's potential to offer tokens with US dollar exposure for self-custody and payments to anyone with a mobile phone and internet connection is a major opportunity to advance financial inclusion—especially in developing countries.

This is evidenced by the unveiling of personal wallet technology in El Salvador this past year, which enabled storage and transfers in both bitcoin and US dollars. The Salvadoran government offered each citizen a free $30 worth of bitcoin if they downloaded a wallet, specifically a mobile one developed by the government, called Chivo Wallet.

As of 2022 January, 4 million users, representing over half the total population in El Salvador, had downloaded the wallet. Comparatively, this is greater than the percentage of adult Salvadorans with a bank account. Furthermore, of those that downloaded a wallet, and also spent the $30 worth of bitcoin supplied by the El Salvadoran government, 39% then continued wallet usage; a percentage we find significant considering the learning curve required to transition from a predominantly cash driven economy.

Interestingly however, this did not necessarily coincide with increased bitcoin adoption, as active user spending, receiving, and depositing activities were more prevalently conducted in dollars as opposed to bitcoin. The Central Bank of El Salvador also reported that the country's share of monthly remittance value received in bitcoin, a use case many suspected would convenience Salvadorans, was limited to just 1.7%.

In this vein, Taro not only has an opportunity to advance access to dollars, but it is also likely that there is a high untapped demand for dollars (especially among those stricken with poverty and capital controls, according to Human Rights Foundation CSO Alex Gladstein and Strike CEO Jack Mallers) riding on crypto rails, available without the need to open a bank account.

While difficult to quantify, the steep rise in crypto dollar activity on Tron, a centralised yet mostly permissionless blockchain designed for speedy and cheap payments, offers fairly convincing evidence. However, we caution this data may also be influenced by other factors, such as strategic volume boosting or speculative DeFi activity.

Figure 14: Growth in Tether (USDT) Daily Transfers and Settlement on Tron

(Note that Founder of Bitrefill Sergej Kotliar mentioned in a recent talk, which we highly recommend, that Tron USDT is the 3rd most prevalent payment method on his app only beaten by on-chain bitcoin and ethereum, suggesting that Tron USDT is indeed exchanged for goods in the real-world economy)

Apart from stablecoins there are also a whole host of more exotic token-based assets that may find a more secure footing on the Bitcoin Network using Taro than on inferior altcoin networks. While we don't have the time to analyse all of them within the scope of this paper, the most obvious ones are assets that are already securitised in today's financial system: Debt, equities, commodities, the list is long, but there are also opportunities for NFTs, tickets, collectibles and all sorts of other tokens.

Ultimately however, we believe Taro finds its most immediate potential in serving unfulfilled dollar demand in regions with harsh financial restrictions or inadequate banking infrastructure. This will likely happen first in areas that have already been exposed to digital wallet technology, such as the early communities in Latin America, Africa, and India.

Censorship Resistance

It is well understood that the censorship resistance property of Bitcoin is a consequence of transaction fees. Therefore, Taro's potential to increase transaction demand on the Bitcoin blockchain, by enabling new types of asset transfers, could strengthen its protection against chain reorganisation attacks.

The codified constraints in both block time and size explicitly limits transaction throughput on the Bitcoin blockchain (hence the ongoing development of scaling technologies Lightning and Liquid) in order to maximise decentralisation. This creates a scarcity of block space which in turn drives the transaction fee market. Here, spenders 'bid' for settlement and miners 'ask' for remuneration in an orderbook-style queue called the mempool.

It is a combination of the free market for block space and the desire for timely settlement that determines the fee levels in the mempool. The more motivated a spender is to ensure timely inclusion of their transaction in a block, the more they will offer miners to include it. Miners that neglect transactions paying competitive fees are at a revenue disadvantage to those that do not. Over time, and on the whole, this drives censoring miners out of the market as they are unable to survive in the highly competitive mining industry.

We find it reasonable that an improved user experience of spending assets on Bitcoin payment rails—especially for stablecoins—will increase Bitcoin transaction demand, and with it, average fee levels.

While we are careful not to imply that Taro will with certainty impact Bitcoin's fee market and make transactions significantly more difficult to censor, we do believe that new projects, if successful, would boost demand for Bitcoin block space. The opportunity could then have a rippling impact on the overall ecosystem, but perhaps most directly, on censorship resistance.

Flexibility

The most obvious opportunity for Taro is increasing economic flexibility for Bitcoin users without having to leave the Bitcoin system. This in turn allows developers to experiment with creating assets of greater breadth and complexity, which if popular would have the consequence of improving the network effect of the Bitcoin monetary system. Some examples of anticipated features we have only briefly mentioned in this report is the ability to issue digital collectibles, derivatives, debt or equities.

We are reluctant to make any hard predictions on the impact new asset creation may have on Bitcoin, especially given many developers that were historically experimenting with customisable assets ended up migrating to alternative cryptocurrency ecosystems. However, we are generally encouraged by developers being handed new creative tools. As we've already noted, the simple addition of US dollars to Lightning payment rails alone has tremendous upside potential.

The major opportunity is enhancing the suite of products and services available for users to spend both bitcoin and alternative assets without having to leave the Bitcoin monetary system. This could have positive impacts on both Bitcoin's censorship resistance property (explained above) and overall network effect (explained below).

Lightning Network Effect

The Lightning Network bases itself on Bitcoin's underlying security model, but rather than limiting its ability to incremental and irreversible final settlement transactions, Lightning is designed for speed and volume with the ability to handle a virtually unlimited number of near instant payments.

Lightning has steadily grown in popularity over time, and is steadily growing its ability to deliver upon its original purpose of improving the scalability of small casual payments within the Bitcoin Monetary System. As a new tool able to deliver payments cheaply and quickly, it has, in our view, greatly enhanced the ease with which bitcoin can be used as a medium of exchange. In other words, Lightning has helped bitcoin better fulfil one of the core functions of money, because it has made it easier to use it as money.

We intentionally point out that Lightning can increase bitcoin's usage specifically as money, because it has an important impact on bitcoin's long-term and fundamental investment case. In our view, as bitcoin grows in usage as money, its monetary premium will also grow, adding incremental exchange value to each unit.

It is fairly well understood today that bitcoin is only suitable as an investment because of the growing usage its monetary properties can attract to it as it competes in the global monetary market. It is these monetary properties that cause people across the globe to find bitcoin useful as money, whether it be due to its scarcity, transferability, durability, or whatever else.

Its usefulness makes different people in different individual situations choose bitcoin over some other competing money, further enhancing its usefulness to others who now observe more people accepting it in exchange for goods and services. Ultimately, this creates a virtuous cycle of network effects, and it causes the bitcoin unit to take on an increasing monetary premium.

Anecdotally, we find there is a strong overlap between long-term investors that understand bitcoin's future value potential as money and those who are using the

Lightning Network as a payments system. Therefore, almost counterintuitively, we do not expect very significant payments growth on the Lightning Network in the short-term. This is because a large number of bitcoin users consider bitcoin a superior form of money and therefore use it for saving, instead preferring to spend inferior fiat (as Gresham's Law eloquently puts it: bad money drives out good).

However, in the case Taro is successful, the addition of alternative monies to the Lightning payments system would offer users, both existing and new, the choice of which asset(s) to spend and which asset(s) to save, all within the highly secure, permissionless and censorship resistant Bitcoin monetary system.

The increased utility on Lightning may then play into its own form of a virtuous cycle of network effects, where its usefulness makes users choose Lightning over some other competing payment platform. This will then further enhance its usefulness to others who now observe more users available for trade via cheap and near instant transactions within its network.

Figure 15: Flywheel of Lightning Network Effects

We also suspect that if Taro has the effect of improving the attractiveness of Lightning for both users and businesses it could also improve the earnings potential of routing providers and perhaps enhance the market for borrowing Lightning liquidity. The effect here could come both in terms of the possible returns on capital for lightning liquidity providers—itself a potential driver of network infrastructure investment— and the potential market opportunity of issuing new Lightning assets.

Lastly, the onboarding of new users to the Lightning network could be a catalyst that spreads the idea of bitcoin to a new group of potential adopters who have not yet explored its potential and properties as money. This may be the most challenging opportunity for Taro, however it is also potentially the most impactful for bitcoin, its value, and the path it takes in competing with other forms of money.

Privacy

The privacy properties of Taro transactions, and by extension any Taro assets contained within them are strong and applied by default. That is, no specific action is required on the part of users to take advantage of the privacy properties of Taro assets. As mentioned in Section 5 of this report however, users may choose to forego certain privacy benefits by sharing their transaction data with interested parties. This would only be done on a voluntary basis.

Taro transactions are contained within Taproot transactions, meaning that general blockchain observers will be unable to determine if a bitcoin transaction contains a Taro asset. Furthermore, under the assumption that Lightning Taro transactions have the same privacy as Lightning bitcoin transactions, only the transactors themselves will be aware that any Taro payment occurs, and the history will not be recorded on the underlying Bitcoin blockchain.

We are therefore optimistic that Taro transactions will have the opportunity to enjoy the same privacy capabilities of existing Taproot and Lightning transactions. We are however cautious that should users be comfortable with sharing their transaction data, the availability of services similar to block explorers may enable blockchain-like visibility into the transaction activity of certain Taro assets.

Major Taro Risks

Technical Complexity

Taro is the result of creative engineering with relatively new technologies. As a result, users should expect that applications leveraging Taro will not be bulletproof from the very beginning. Proper development is a time-consuming process.

The underlying technology of Taro, Taproot, is still in the process of being fully supported by most wallet softwares (see status, here), and general usage levels remain low. Only around 0.09% of all bitcoin is stored in P2TR addresses.

This isn't particularly concerning, but is still good to note. It's common for newly activated Bitcoin features to sit idle as developers build proper tooling. We also consider the main benefit of Taproot to be the enabling of higher complexity transactions at lower financial costs. Therefore, new specifications that implement Taproot, such as Taro, may be necessary to catalyse significant levels of development and usage.

For most however, the ability to make Taro payments will depend on wallet developers creating usable and secure wallet implementations of Taproot, which have the added functionality to recognise and spend Taro assets. It's not hard to imagine this taking several years and extensive testing before consumer usage becomes widespread.

Many of the major opportunities of Taro also depend on its compatibility and effectiveness on the Lightning Network. Therefore, the success of Taro will likely depend on general Lightning reliably and the additional infrastructure required to cheaply deliver Taro assets.

And while perhaps obvious, just as the dependency on Lightning introduces some level of risk to Taro assets, so does its dependency on final settlement on the Bitcoin blockchain. As a result, any potential problems suffered by these systems will also have a negative impact on Taro services.

Ultimately, users are not simply introduced to the technology risk of a particular Taro application, but also to the components that application depends upon, such as wallet providers, the Lightning Network and the Bitcoin settlement process.

Dependencies

While the technical dependencies described above are the same for any software leveraging Lightning and Taproot, other dependencies may arise from the specific participants that support each Taro asset.

At the end of the day, the only asset that can be transacted on the Bitcoin and Lightning Networks, without any reliance on a third party, is bitcoin. Whenever another asset is represented and tokenised within these networks, there will *necessarily* arise a dependency on a third party. This may be an exchange, an issuer, an index etc.

The most simple example of third party dependency is the issuer that operates the creation and redemption mechanism of each asset. Another example would be entities providing the data sources of outside data such as exchange rates (referred to as oracles).

Serviced data may be misleading or incomplete in certain circumstances, and in such cases, what is the proper recourse? Or, what are the incentives of each party involved? There are many as of yet unsolved problems at the intersection between third parties and decentralised networks, and this may have to be an area where recourse to legal systems could be required.

Failures of data feeds or connected markets could cause pricing issues, failure of asset issuers or custodians could cause redemption issues. Many of the potential issues that might arise are the same as those that have been faced by the securities industry for decades already, so we expect that inspiration and evolution from that sector will be instrumental in getting these issues solved.

Overall, we find that each Taro asset and any supporting entities will introduce different categories and varying degrees of third party dependencies. Mindful investors should be careful to evaluate the players involved and assess each asset in accordance with their risk tolerance, especially during the earliest stages of Taro deployment.

Regulation

The above section leads us right down the path of potential regulation. As mentioned, all Taro assets will have some third party dependencies, and users, having no recourse within the rules of the Bitcoin protocol itself may seek alternative protection through existing or newly developed legal frameworks within specific jurisdictions.

The current guidelines under which the cryptocurrency industry operates are often ambiguous, not having been designed with crypto assets in its purview, leaving room for shady players to take advantage of overly trusting clients. On the flip side, uncertainty and unfavourable laws and compliance mandates that were designed for a mature securities industry could be applied to startup crypto projects and carry repercussions that might potentially weaken or even stop certain projects dead in their tracks.

While Taro simply being an open-source software package limits the abilities of authorities to forcibly prevent assets from being issued and transacted, intervention by authorities may disrupt registered businesses within their jurisdiction and infrastructure that are built around it, making assets issued on Taro reasonably vulnerable to adverse regulation.

It is also reasonable to expect that many potential users would *want* recourse to a legal system within some trustworthy jurisdiction in order to be comfortable owning and trading tokenised assets. Many of the current largest holders and transactors of securities will simply be unable to interact with Taro assets in the absence of clear legal and regulatory frameworks.

We'll round off this section by noting that several of the asset classes one can envision being tokenised using protocols such as Taro seem to fall pretty squarely into many countries' current classifications of securities. We fully expect regulators to vocally engage with Taro issuers should they be of the opinion that this is indeed the case. This would likely be damaging to innovation and increase the barriers of entry for startups, but at the same time, if issuers are able to comply with regulations, it could also open the door for a vastly larger user base than would otherwise be possible to attract.

Community Discouragement

Just as with prior asset issuance protocols, Taro may find itself rejected by a community that has historically chosen to limit protocol flexibility in the tradeoff against feature richness. Community indifference is likely also the path of least resistance, being that Taro's success will certainly depend on groups of developers building the tools necessary for it to evolve beyond a conceptual design scheme. If Taro fails to generate excitement and developer interest, it might wither on the vine.

Social disapproval may also be exacerbated by sensationalised failures or early scam attempts by bad actors leveraging the Taro protocol. As we have witnessed in the broader cryptocurrency ecosystem, dishonest developers and speculative companies that deceive investors into unstable or outright fraudulent investments have adverse reputational effects on the underlying technology (recent examples: Celsius, Terra). However, the continued popularity of Ethereum given the enormous amount of scams and hacks within its ecosystem might suggest our concern on the matter may be overblown.

In the Bitcoin ecosystem, this sort of deception has mostly been limited to faulty exchanges and cloud mining scams—all centralised projects *connecting to* Bitcoin, not so much projects building directly on top of Bitcoin's protocol stack. Still, the flexibility of Taro (listed previously also as an opportunity) will reduce the friction for developers to issue dishonest assets. This could become a reputational issue over time, causing rejection and discouragement by the general Bitcoin community.

Costliness

Bitcoin network participants who voluntarily enforce the additional rules of Taro will be required to expend more computational resources (bandwidth, storage, etc.) than those who do not. While this specifically does not impact the existing Bitcoin ecosystem, it may introduce certain centralisation risk to the Taro ecosystem, where particular assets may be confined to a small set of issuers, data providers, or Lightning routers.

Of particular concern to us are the potential resources required to generate, relay, and store Taro ownership proofs, which increase linearly in size with each additional on-chain transaction. Each Taproot transaction involving Taro assets encumbers a newly created proof containing all previous ownership states since the Taro assets were issued.

Therefore, Taro proofs may become very large in the future, increasing the cost of participants transacting these assets. Without efficiency improvements in packaging and transferring Taro data, these costs could either reduce the set of participants supporting the Taro ecosystem, reducing usefulness of the transaction network and therefore the desirability of the asset.

We also suspect Taro asset payments will likely be more costly than bitcoin payments on the Lightning network, due to both a decreased competitive environment and the likelihood that payment routers would seek to remain market neutral.

Entities that serve as intermediaries between general Lightning members and Taro-enabled members will have varying degrees of asset exposure to facilitate swaps along payment routes. We find it likely that these entities will charge spenders the cost of hedging their exposure to the Taro assets they have chosen to support. As a result, Taro payments may be subject to fees similar to or larger than that of spot exchange markets, and be subject to spreads that are larger than those found in centralised marketplaces.

Influence on Bitcoin Governance

The use of Bitcoin second layer technologies such as the Lightning Network and Sidechains can introduce a number of risks when it comes to fork outcomes. The decentralised nature of the Bitcoin network means that the ultimate decision of which chain to support lies with the economic actors in the network. This can be problematic since the decisions of heavy economic actors, such as exchanges, or potentially large Taro owners or issuers, could conceivably influence fork selection processes.

For example, if exchanges were to support one chain over the other, this could lead to a divergence in the overall chain selection of Bitcoin users, ultimately resulting in a split in the network.

The underlying issue here is that users of Taro assets on bitcoin may be heavy economic entities in terms of fork outcome selection, but they may not be heavy bitcoin owners, causing a divergence in incentives. Since a Taro user fundamentally owns something *outside* of bitcoin, and probably has some recourse to those assets should bitcoin fail, they may not be properly incentivised to participate in bitcoin governance, leading to perversions in the governance processes.

At the end of the day, it will continue to be the economic weight that matters in bitcoin governance. And while we believe that this is a potential issue that should be closely observed, if it becomes a major distorting factor in bitcoin governance there are always steps that could be taken to mitigate or remove the problem.

Notes

[1] The earliest asset issuance projects used unspendable multisignature outputs that bloated the UTXO set, causing higher memory requirements for network members to the extent Bitcoin developers implemented a specific function (known as Op_Return) as a custom data slot in transactions to reduce tension. Although, these Op_Return transactions were also, and for the most part remain, controversial for increasing the blockchain size and Bitcoin's storage requirements.

[2] The higher the proportion of Taproot transactions being spent on the blockchain, the harder it becomes to guess whether any of them contain Taro assets. Once the so-called anonymity set gets large enough, guessing becomes practically impossible.

[3] Payment channels are a clever technique that uses one opening, and one final settlement transaction, to encompass many historical trades. They work similar to a pre-funded tab of sorts, where two entities continuously track a history of payments as they're streamed back and forth, or even hop between multiple connected users to reach counterparties that are not *directly* connected. Then, upon deciding to conclude their trading partnership, they submit the final balance to the Bitcoin blockchain and undergo its robust settlement process.

[4] Taro nodes must run one of the newer versions of Bitcoin's protocol rules, one that's been released since the Taproot activation in November 2021.

Disclosure

The information contained in this document is for general information only. Nothing in this document should be interpreted as constituting an offer of (or any solicitation in connection with) any investment products or services by any member of the CoinShares Group where it may be illegal to do so. Access to any investment products or services of the CoinShares Group is in all cases subject to the applicable laws and regulations relating thereto.

This document is directed at professional and institutional investors. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. This document contains historical data. Historical performance is not an indication of future performance and investments may go up and down in value. You cannot invest directly in an index. Fees and expenses have not been included.

Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to.This document fairly represents the opinions and sentiments of CoinShares, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and / or obtained from sources believed to be reliable; however, CoinShares does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the date indicated. Third party data providers make no warranties or representation of any kind in relation to the use of any of their data in this *document. CoinShares does not accept any liability whatsoever for any direct, indirect or consequential loss arising from any use of this document or its contents.*

Any forward-looking statements speak only as of the date they are made, and CoinShares assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time. Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

This document is directed at, and only made available to, professional clients and eligible counterparties. For UK investors: CoinShares Capital Markets (UK) Limited is an appointed representative of Strata Global Limited which is authorised and regulated by the Financial Conduct Authority (FRN 563834). The address of CoinShares Capital Markets (UK) Limited is 82 Baker Street, London, W1U 6TE. For EU investors: CoinShares AM (napoleon-am.com) is a French asset management company regulated by the Autorité des Marchés Financiers (AMF), registered under number GP-19000015 since 27/03/2019. Its office is located at 25 rue du 4 Septembre, 75002 Paris, France.

The CoinShares Astronaut is a trademark and service mark of CoinShares International Limited.

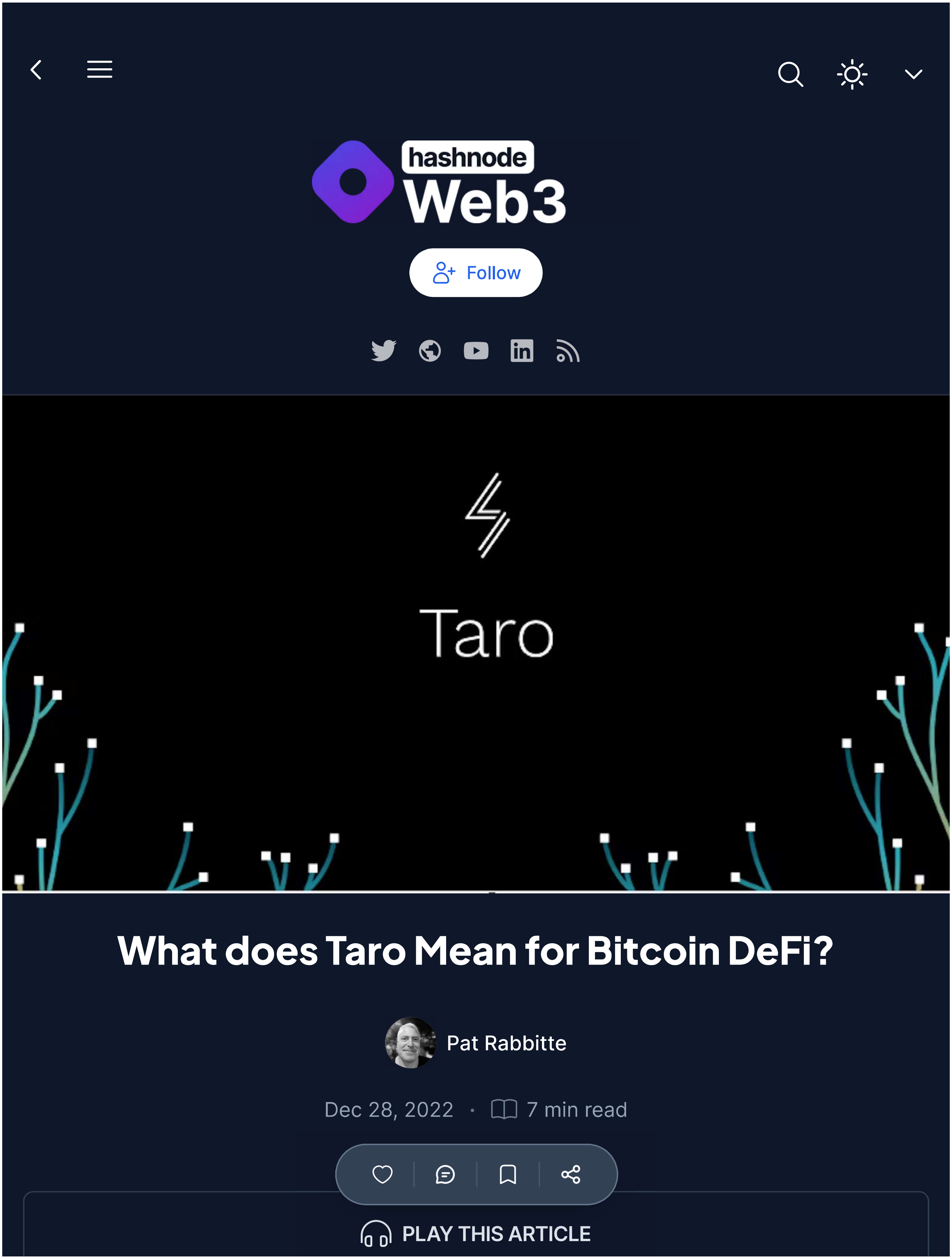
CoinShares

CONTACT US

CAREERS

DISCLAIMER

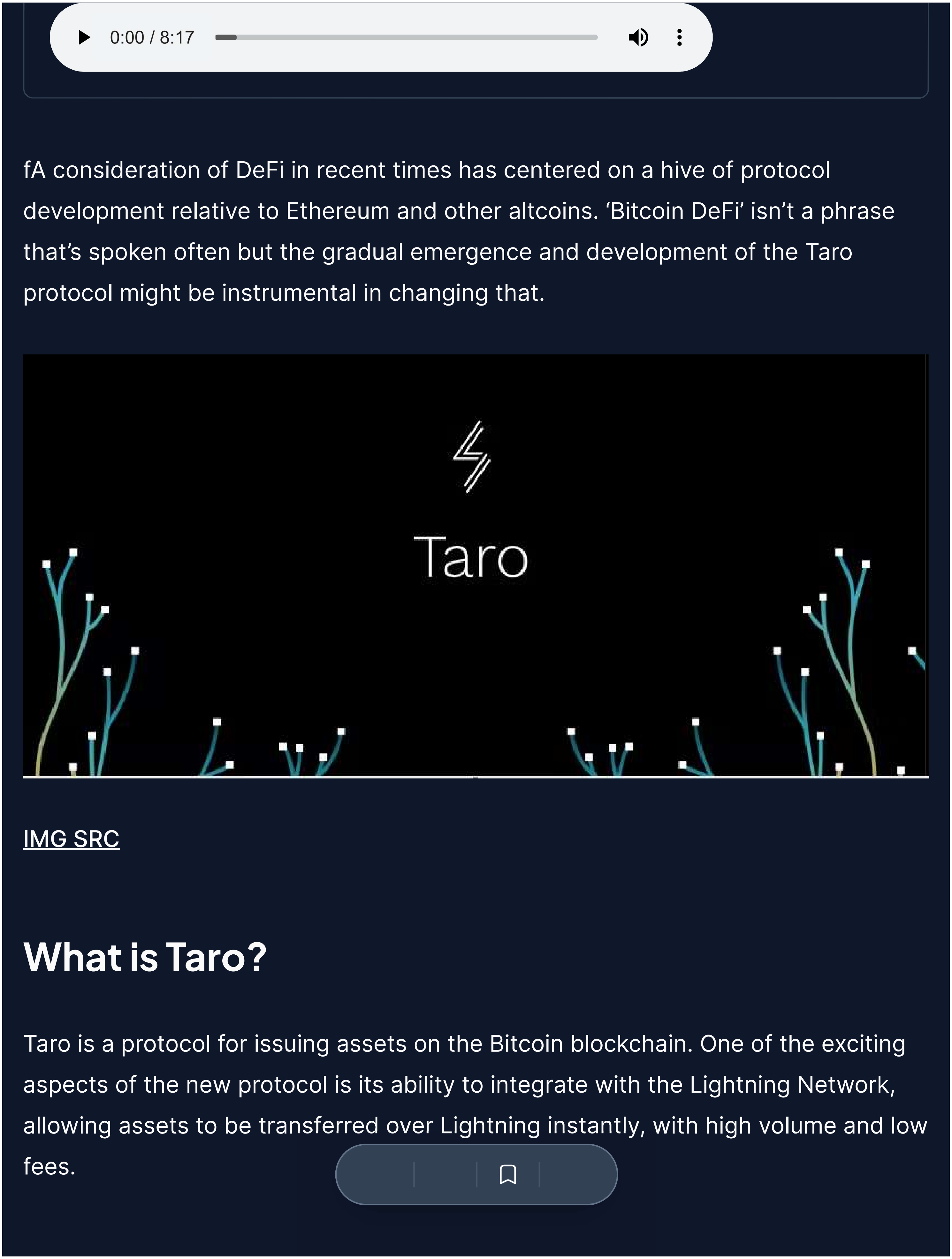
PRIVACY POLICY



What does Taro Mean for Bitcoin DeFi?

Pat Rabbitte

Dec 28, 2022 · 7 min read



fA consideration of DeFi in recent times has centered on a hive of protocol development relative to Ethereum and other altcoins. ‘Bitcoin DeFi’ isn’t a phrase that’s spoken often but the gradual emergence and development of the Taro protocol might be instrumental in changing that.

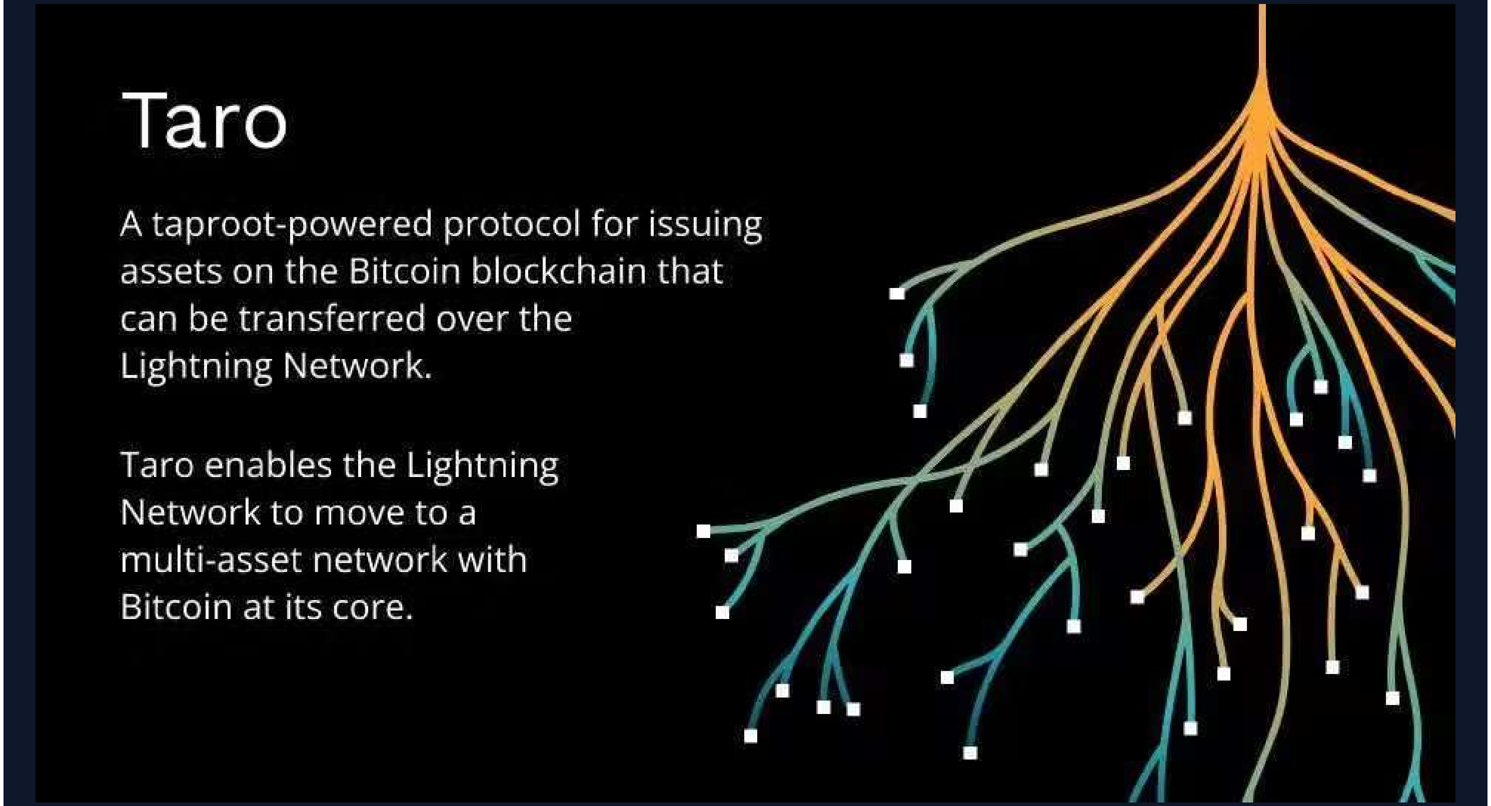
IMG SRC

What is Taro?

Taro is a protocol for issuing assets on the Bitcoin blockchain. One of the exciting aspects of the new protocol is its ability to integrate with the Lightning Network, allowing assets to be transferred over Lightning instantly, with high volume and low fees.

Taro is an abbreviation for Taproot Asset Representation Overlay. The protocol is the result of bitcoin improvement proposals (BIP) advanced by Lightning Network development firm, Lightning Labs.

This is not the first attempt to bring other digital assets to the Bitcoin blockchain. The difference between Taro and other efforts is that it relies on the functionality added via Bitcoin's last major upgrade, Taproot.



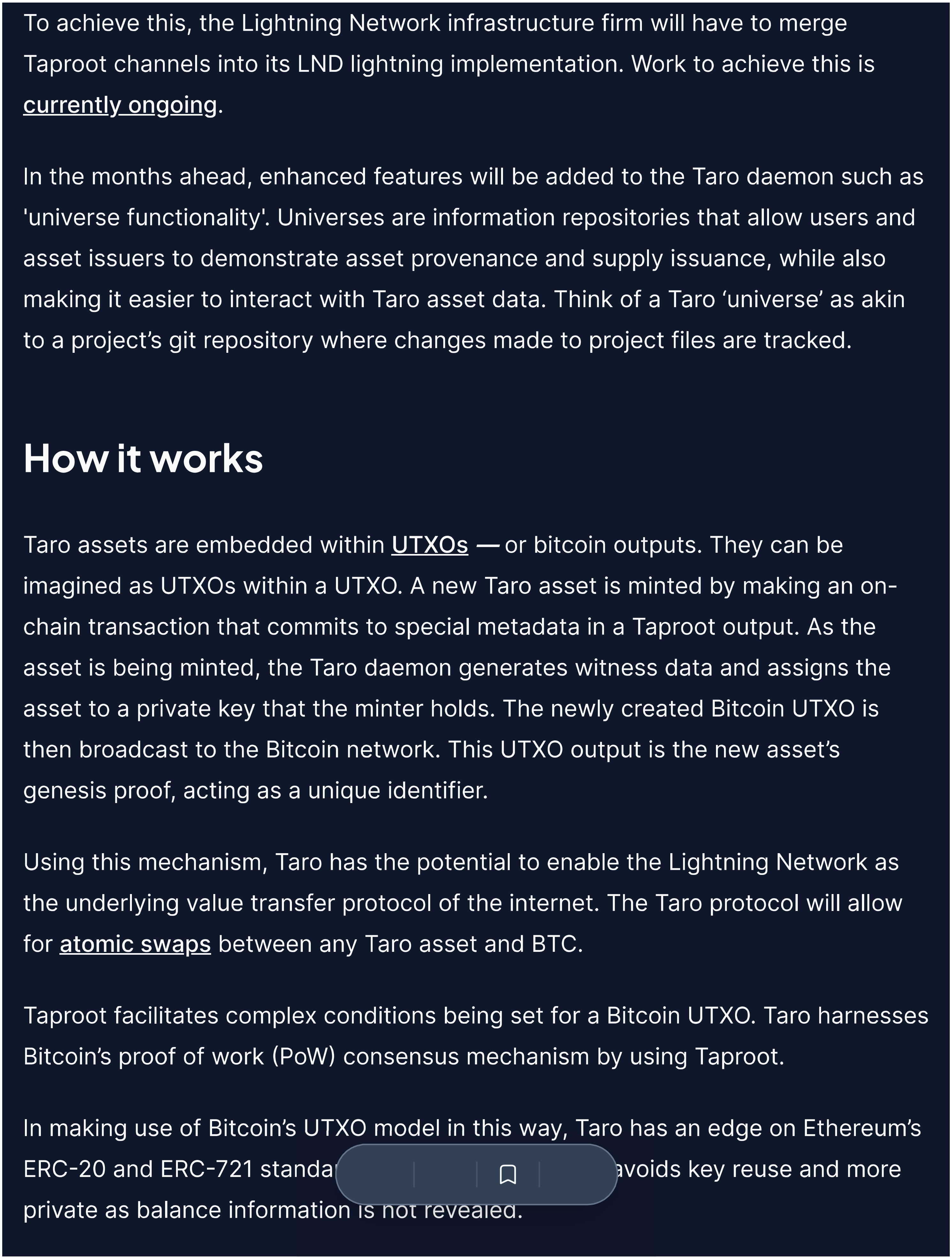
Taro

A taproot-powered protocol for issuing assets on the Bitcoin blockchain that can be transferred over the Lightning Network.

Taro enables the Lightning Network to move to a multi-asset network with Bitcoin at its core.

IMG SRC

Lightning Labs released the first version of Taro in September. This initial alpha release has gone live on testnet as a precursor to eventually going live on the Bitcoin mainnet once any bugs have been ironed out. Lightning Labs stated that integration with Lightning Network is included in the developmental roadmap for Taro and will be added in the future.



To achieve this, the Lightning Network infrastructure firm will have to merge Taproot channels into its LND lightning implementation. Work to achieve this is currently ongoing.

In the months ahead, enhanced features will be added to the Taro daemon such as 'universe functionality'. Universes are information repositories that allow users and asset issuers to demonstrate asset provenance and supply issuance, while also making it easier to interact with Taro asset data. Think of a Taro ‘universe’ as akin to a project’s git repository where changes made to project files are tracked.

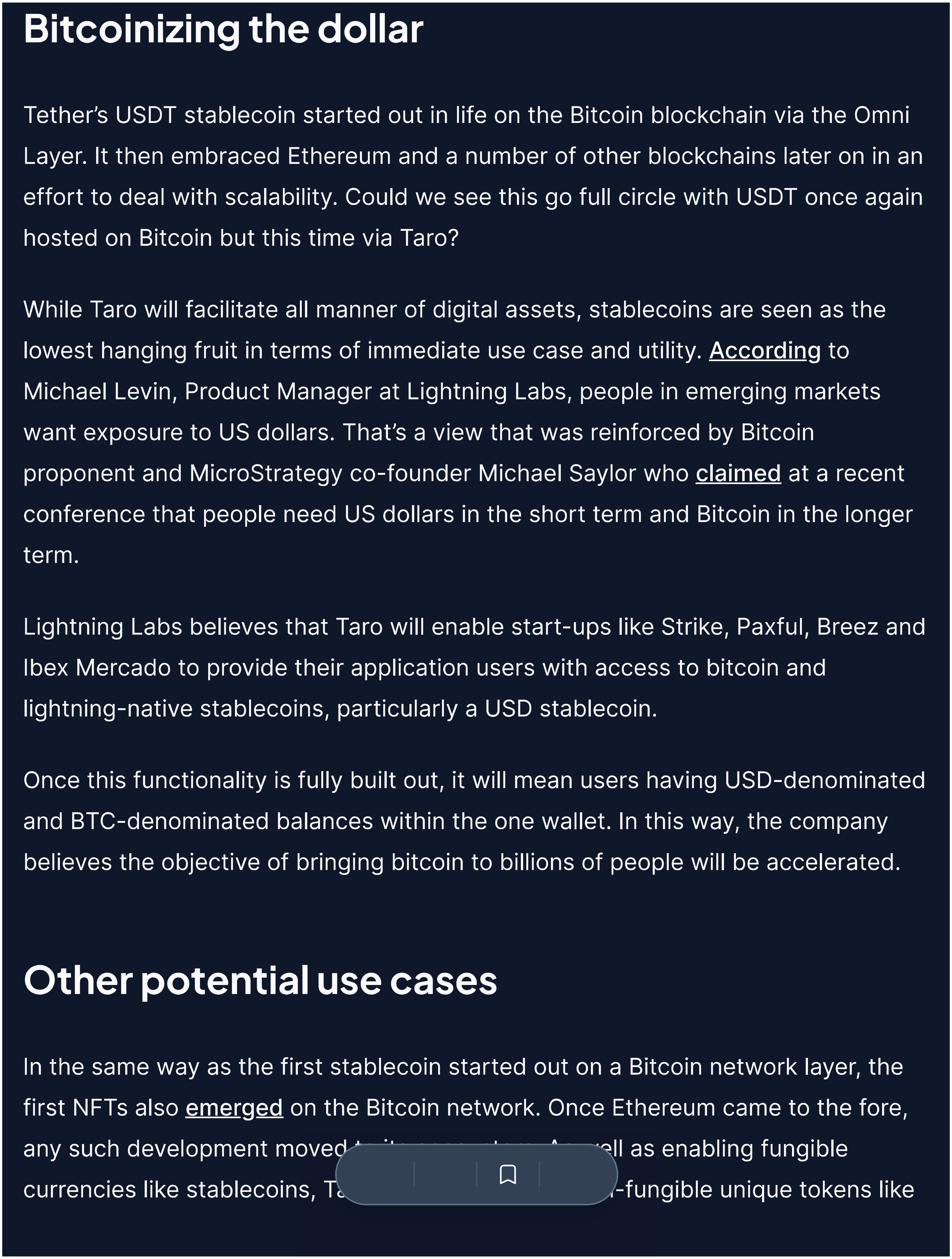
How it works

Taro assets are embedded within UTXOs — or bitcoin outputs. They can be imagined as UTXOs within a UTXO. A new Taro asset is minted by making an on-chain transaction that commits to special metadata in a Taproot output. As the asset is being minted, the Taro daemon generates witness data and assigns the asset to a private key that the minter holds. The newly created Bitcoin UTXO is then broadcast to the Bitcoin network. This UTXO output is the new asset’s genesis proof, acting as a unique identifier.

Using this mechanism, Taro has the potential to enable the Lightning Network as the underlying value transfer protocol of the internet. The Taro protocol will allow for atomic swaps between any Taro asset and BTC.

Taproot facilitates complex conditions being set for a Bitcoin UTXO. Taro harnesses Bitcoin’s proof of work (PoW) consensus mechanism by using Taproot.

In making use of Bitcoin’s UTXO model in this way, Taro has an edge on Ethereum’s ERC-20 and ERC-721 standa avoids key reuse and more private as balance information is not revealed.



Bitcoinizing the dollar

Tether's USDT stablecoin started out in life on the Bitcoin blockchain via the Omni Layer. It then embraced Ethereum and a number of other blockchains later on in an effort to deal with scalability. Could we see this go full circle with USDT once again hosted on Bitcoin but this time via Taro?

While Taro will facilitate all manner of digital assets, stablecoins are seen as the lowest hanging fruit in terms of immediate use case and utility. According to Michael Levin, Product Manager at Lightning Labs, people in emerging markets want exposure to US dollars. That's a view that was reinforced by Bitcoin proponent and MicroStrategy co-founder Michael Saylor who claimed at a recent conference that people need US dollars in the short term and Bitcoin in the longer term.

Lightning Labs believes that Taro will enable start-ups like Strike, Paxful, Breez and Ibex Mercado to provide their application users with access to bitcoin and lightning-native stablecoins, particularly a USD stablecoin.

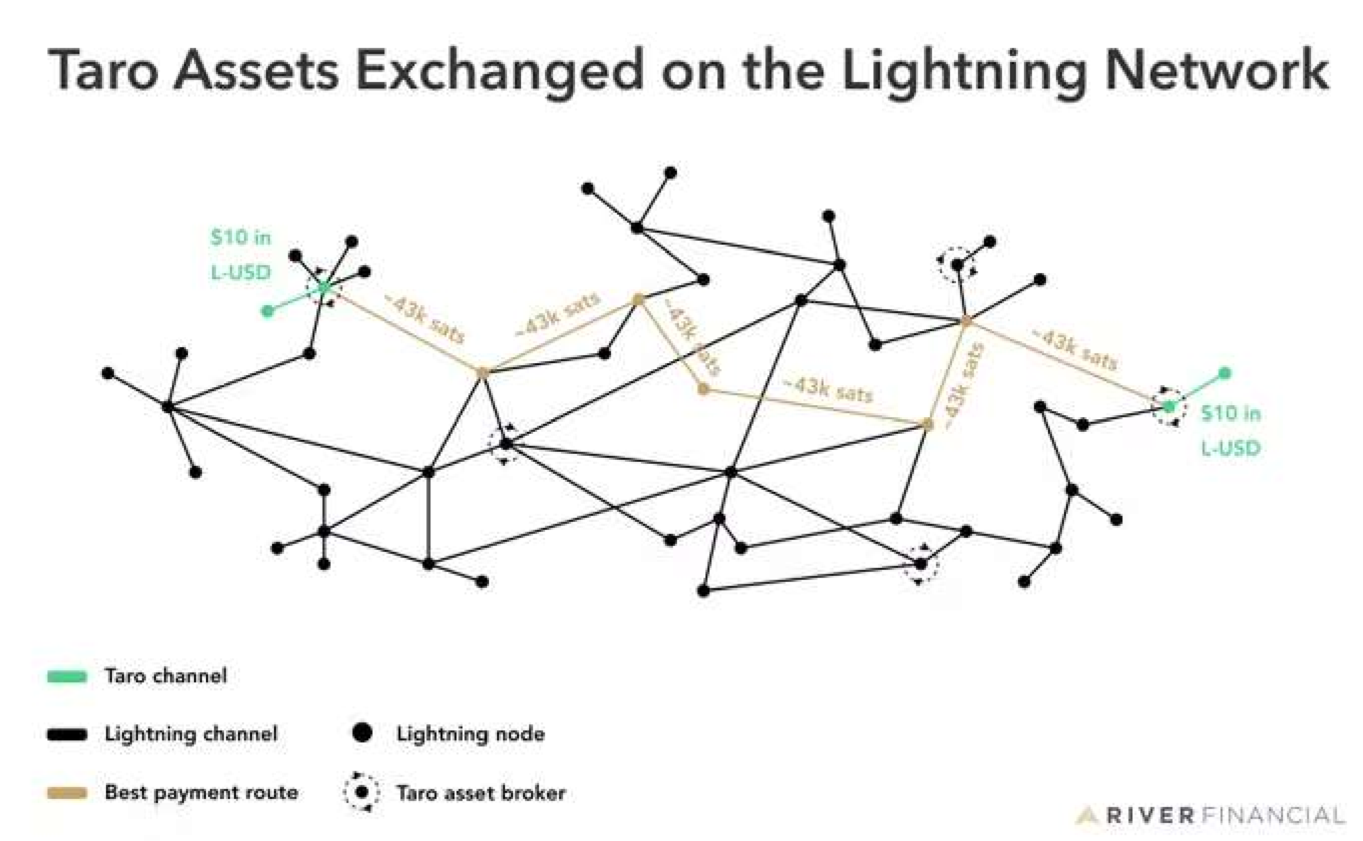
Once this functionality is fully built out, it will mean users having USD-denominated and BTC-denominated balances within the one wallet. In this way, the company believes the objective of bringing bitcoin to billions of people will be accelerated.

Other potential use cases

In the same way as the first stablecoin started out on a Bitcoin network layer, the first NFTs also emerged on the Bitcoin network. Once Ethereum came to the fore, any such development moved ell as enabling fungible currencies like stablecoins, Ta -fungible unique tokens like collectibles or NFTs. It's interesting to think that the potential at least exists through Taro for NFTs to once again feature within the Bitcoin ecosystem.

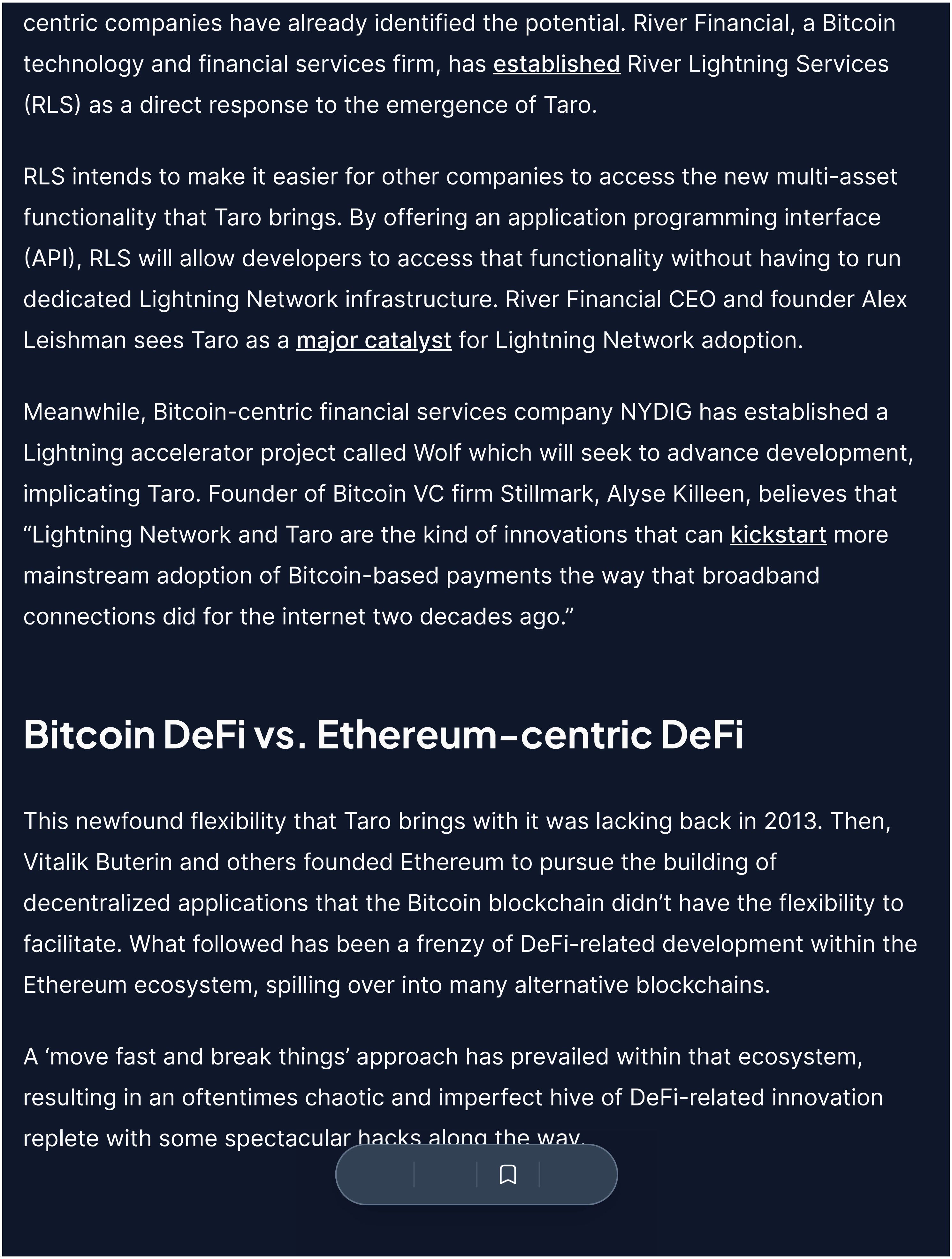
Wrapped altcoins could also feature within the Bitcoin ecosystem via Taro should anyone have the will to create them. There could be a rationale for doing so in leveraging the security of the Bitcoin network.

This initial version of Taro utilizes a level of programmability similar to that of Bitcoin Script. That provides a familiar segue for developers who are already accustomed to Bitcoin Script to build on the new protocol. However, the protocol allows the flexibility to add new opcodes and additional functionality to meet new use cases as they emerge.



IMG SRC

What that demonstrates is th o come from Taro but we still don't know all of the use cases that will be uncovered just yet. Some Bitcoin-



centric companies have already identified the potential. River Financial, a Bitcoin technology and financial services firm, has established River Lightning Services (RLS) as a direct response to the emergence of Taro.

RLS intends to make it easier for other companies to access the new multi-asset functionality that Taro brings. By offering an application programming interface (API), RLS will allow developers to access that functionality without having to run dedicated Lightning Network infrastructure. River Financial CEO and founder Alex Leishman sees Taro as a major catalyst for Lightning Network adoption.

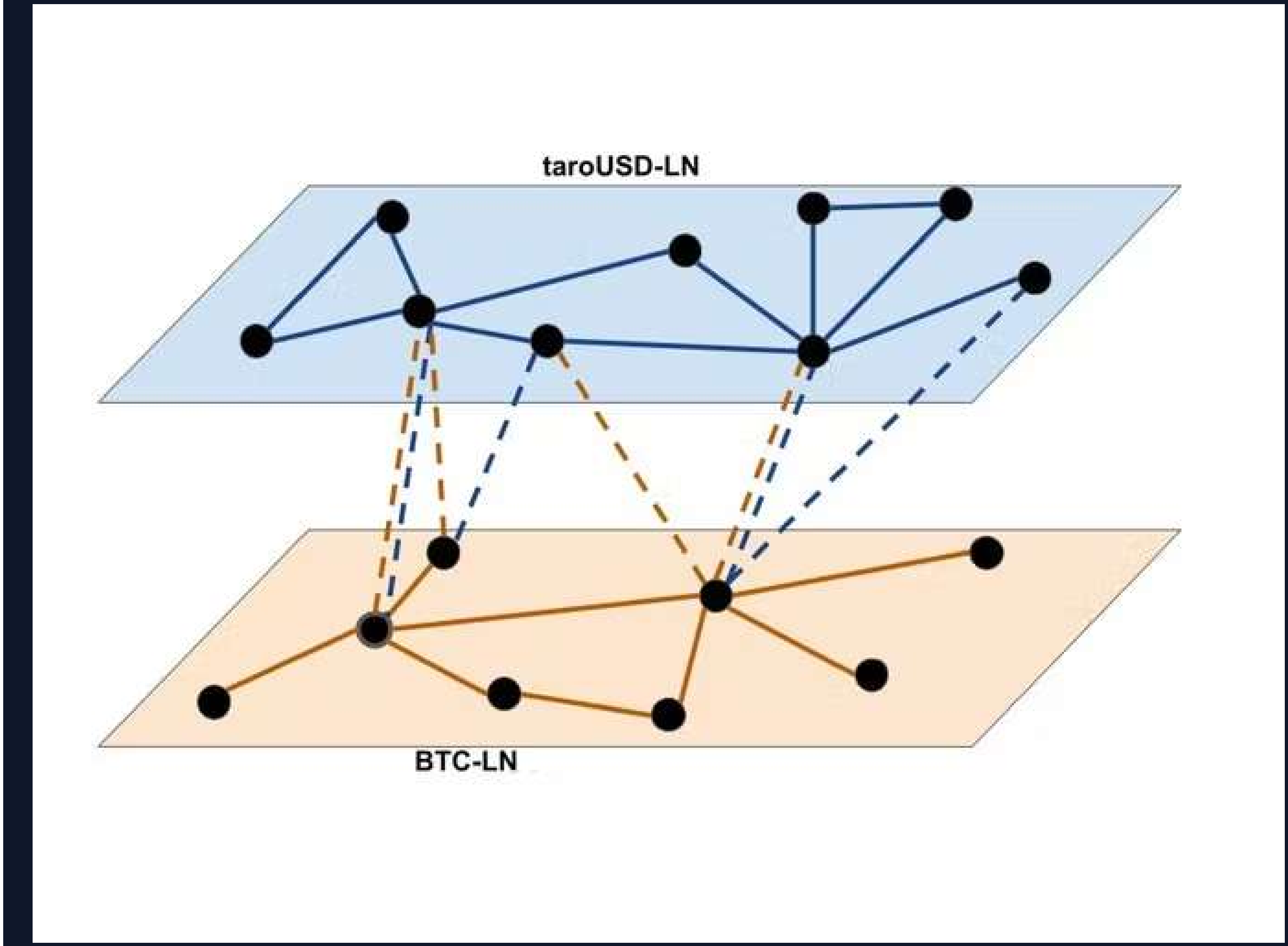
Meanwhile, Bitcoin-centric financial services company NYDIG has established a Lightning accelerator project called Wolf which will seek to advance development, implicating Taro. Founder of Bitcoin VC firm Stillmark, Alyse Killeen, believes that “Lightning Network and Taro are the kind of innovations that can kickstart more mainstream adoption of Bitcoin-based payments the way that broadband connections did for the internet two decades ago.”

Bitcoin DeFi vs. Ethereum-centric DeFi

This newfound flexibility that Taro brings with it was lacking back in 2013. Then, Vitalik Buterin and others founded Ethereum to pursue the building of decentralized applications that the Bitcoin blockchain didn’t have the flexibility to facilitate. What followed has been a frenzy of DeFi-related development within the Ethereum ecosystem, spilling over into many alternative blockchains.

A ‘move fast and break things’ approach has prevailed within that ecosystem, resulting in an oftentimes chaotic and imperfect hive of DeFi-related innovation replete with some spectacular hacks along the way.

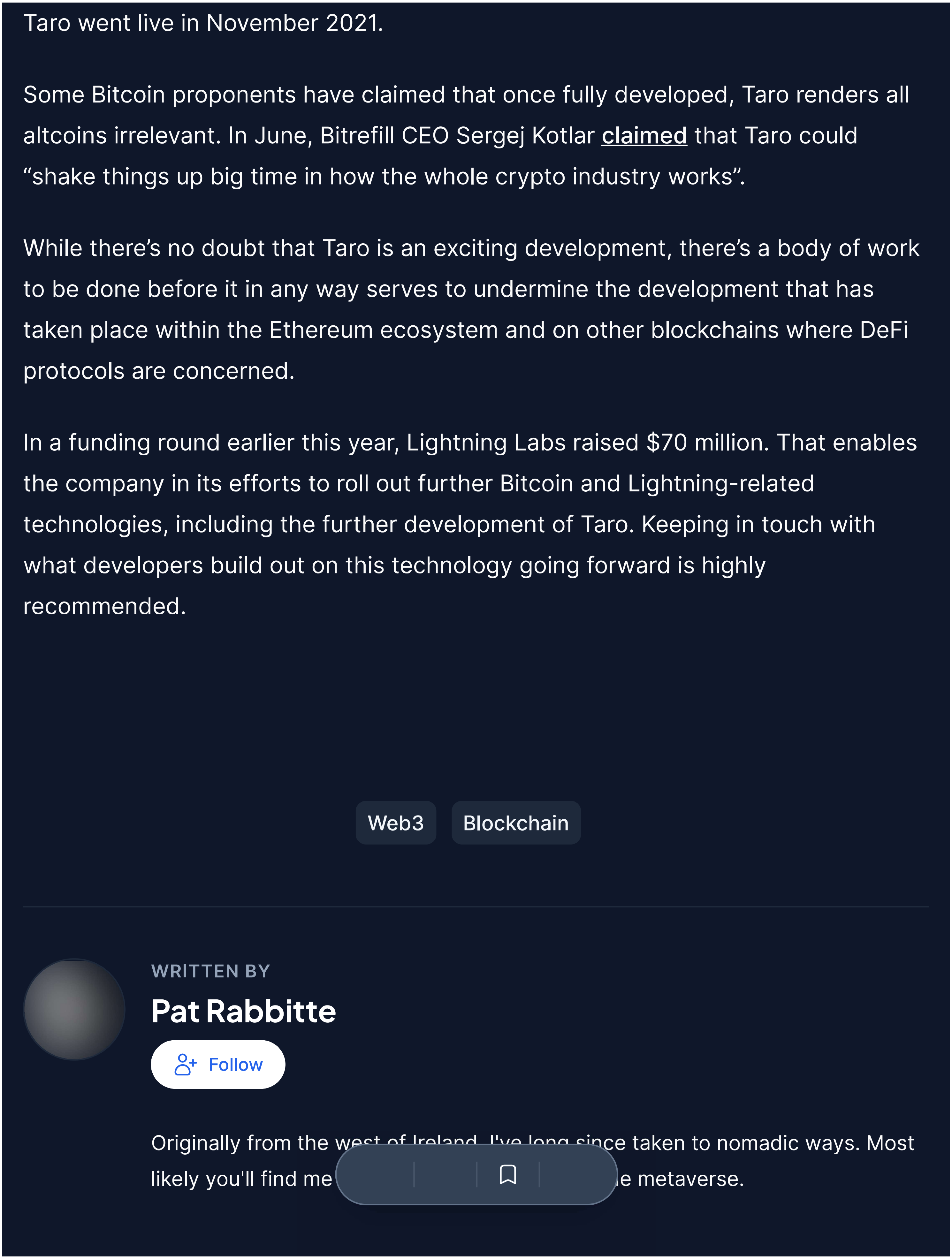
By comparison, development within the Bitcoin ecosystem has been slow. Bitcoin itself has been limited in what it offers developers as Bitcoin Script limits the complexity of what can be built. Developers who have long since moved over to work on other blockchains have bemoaned this shortcoming.



Taro protocol as an extension of layered development on Bitcoin: IMG SRC

Meanwhile, those builders who have continued to focus on Bitcoin see Bitcoin's lack of flexibility as a feature and benefit. The thinking is that the codebase behind the base layer money has to be restrictive to lessen the odds of it coming undone through a hack or exploit.

Instead the approach has bee ates in a very slow, conservative and considered manner. The Taproot upgrade which has facilitated



Taro went live in November 2021.

Some Bitcoin proponents have claimed that once fully developed, Taro renders all altcoins irrelevant. In June, Bitrefill CEO Sergej Kotlar claimed that Taro could “shake things up big time in how the whole crypto industry works”.

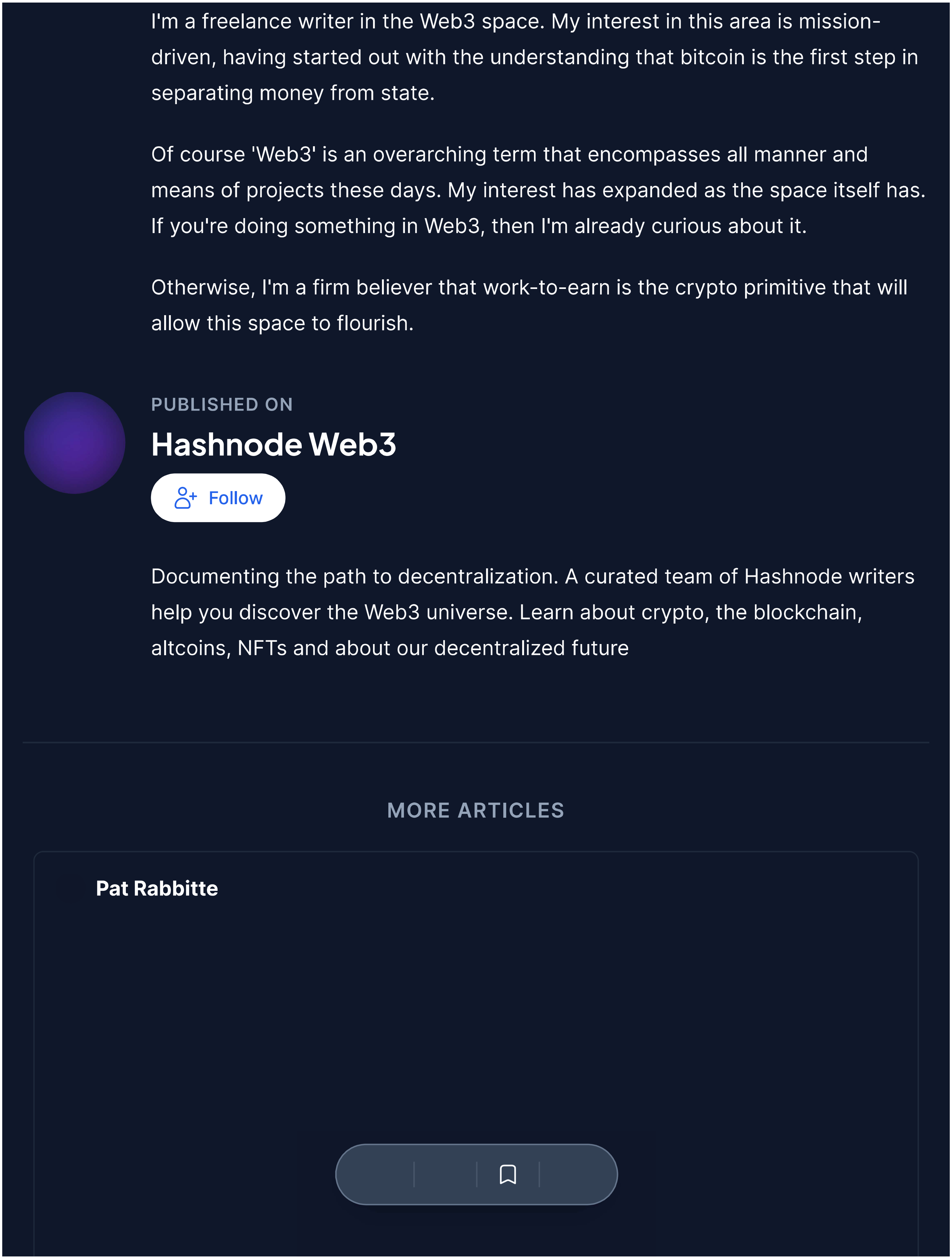
While there’s no doubt that Taro is an exciting development, there’s a body of work to be done before it in any way serves to undermine the development that has taken place within the Ethereum ecosystem and on other blockchains where DeFi protocols are concerned.

In a funding round earlier this year, Lightning Labs raised $70 million. That enables the company in its efforts to roll out further Bitcoin and Lightning-related technologies, including the further development of Taro. Keeping in touch with what developers build out on this technology going forward is highly recommended.

WRITTEN BY

Pat Rabbitte

Originally from the west of Ireland, I've long since taken to nomadic ways. Most likely you'll find me e metaverse.



I'm a freelance writer in the Web3 space. My interest in this area is mission-driven, having started out with the understanding that bitcoin is the first step in separating money from state.

Of course 'Web3' is an overarching term that encompasses all manner and means of projects these days. My interest has expanded as the space itself has. If you're doing something in Web3, then I'm already curious about it.

Otherwise, I'm a firm believer that work-to-earn is the crypto primitive that will allow this space to flourish.

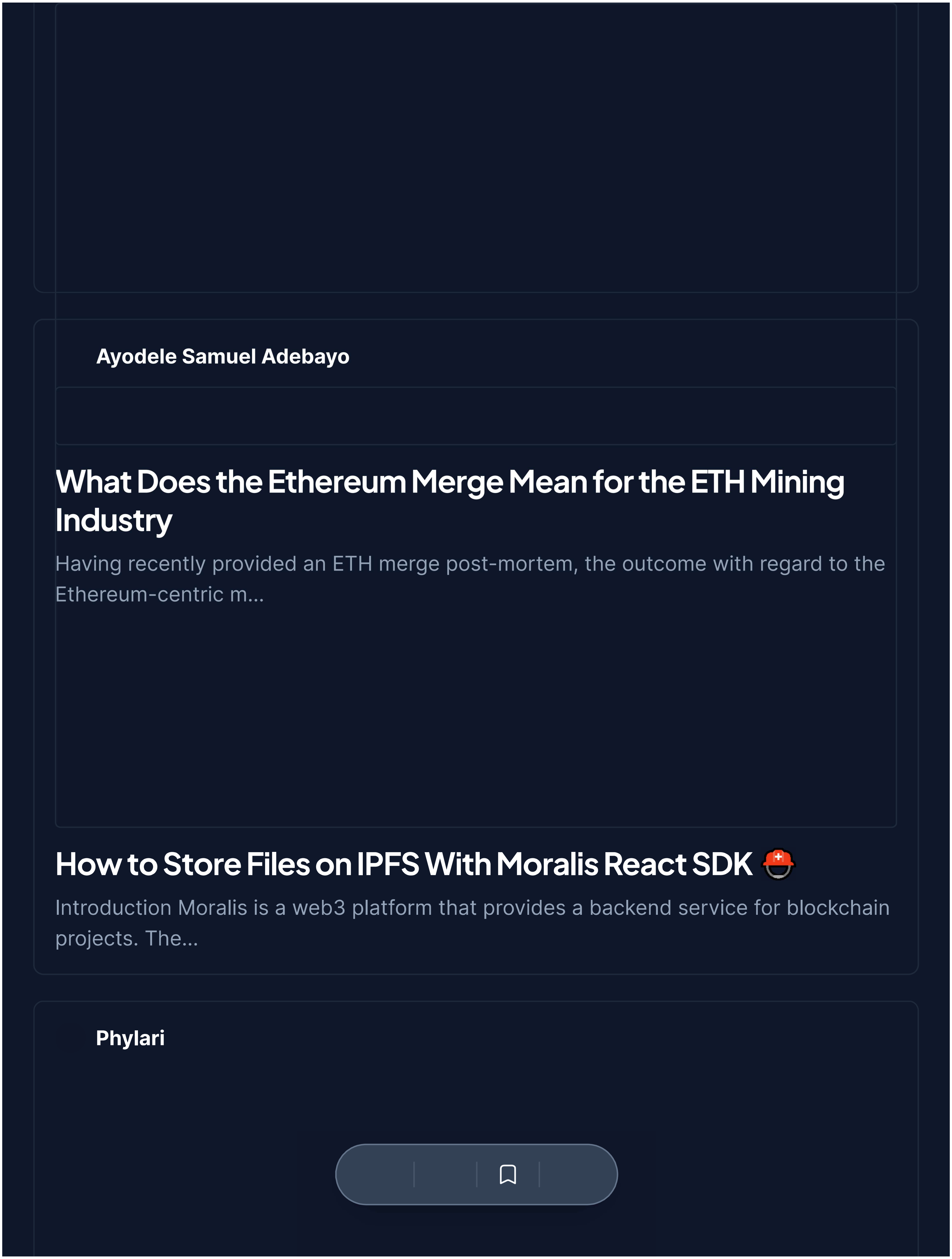
PUBLISHED ON

Hashnode Web3

Documenting the path to decentralization. A curated team of Hashnode writers help you discover the Web3 universe. Learn about crypto, the blockchain, altcoins, NFTs and about our decentralized future

MORE ARTICLES

Pat Rabbitte



Ayodele Samuel Adebayo

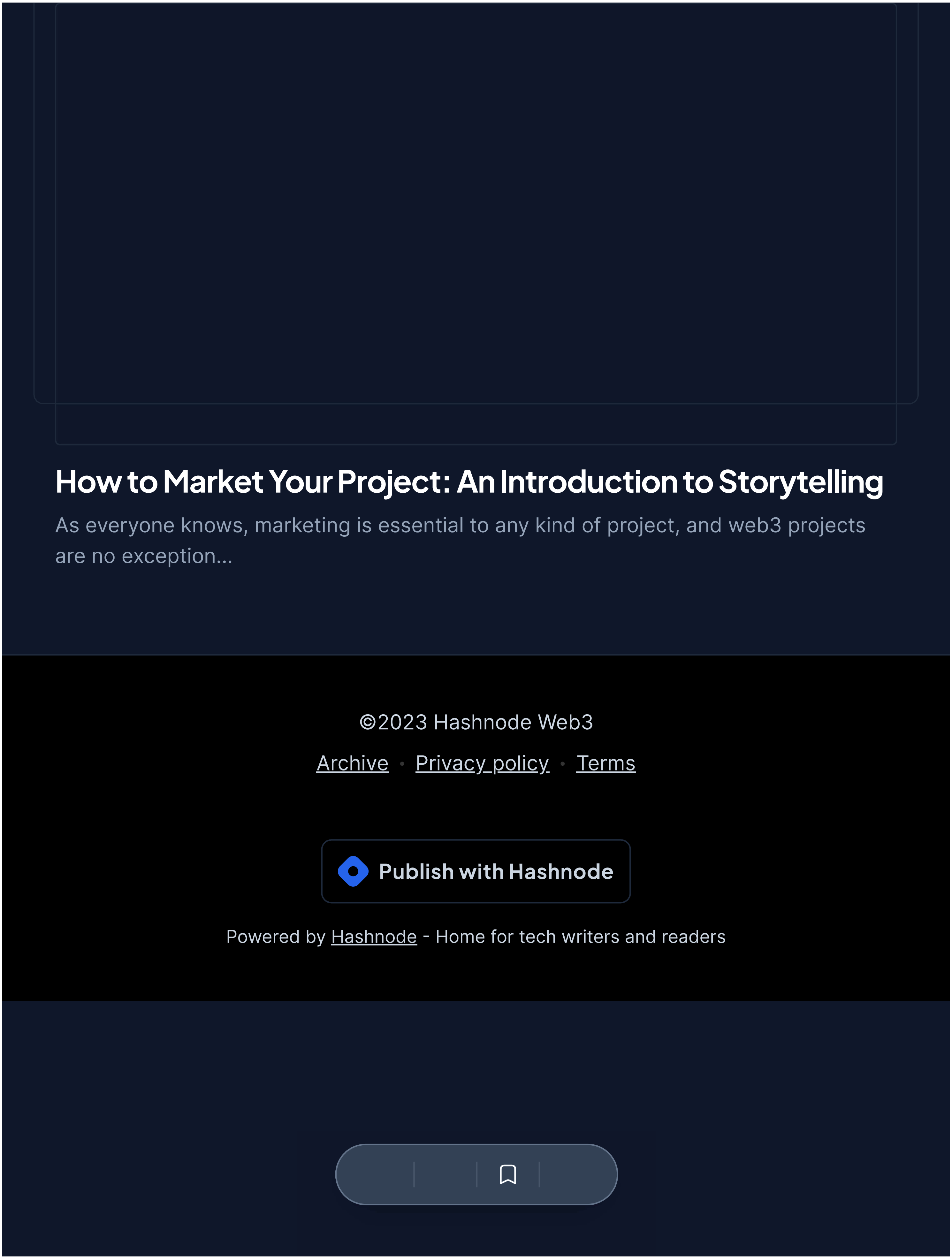
What Does the Ethereum Merge Mean for the ETH Mining Industry

Having recently provided an ETH merge post-mortem, the outcome with regard to the Ethereum-centric m...

How to Store Files on IPFS With Moralis React SDK ⛑️

Introduction Moralis is a web3 platform that provides a backend service for blockchain projects. The...

Phylari



How to Market Your Project: An Introduction to Storytelling

As everyone knows, marketing is essential to any kind of project, and web3 projects are no exception...

Archive · Privacy policy · Terms

Powered by Hashnode - Home for tech writers and readers

BENZINGA Crypto

My Account

SPY	QQQ	BTC/USD	DIA	GLD	TLT
408.33 ▼ 1.36%	303.30 ▼ 1.88%	24472.31 ▲ 1.5572%	337.40 ▼ 1.25%	170.79 ▼ 0.06%	101.59

Search Tickers, Companies or News...

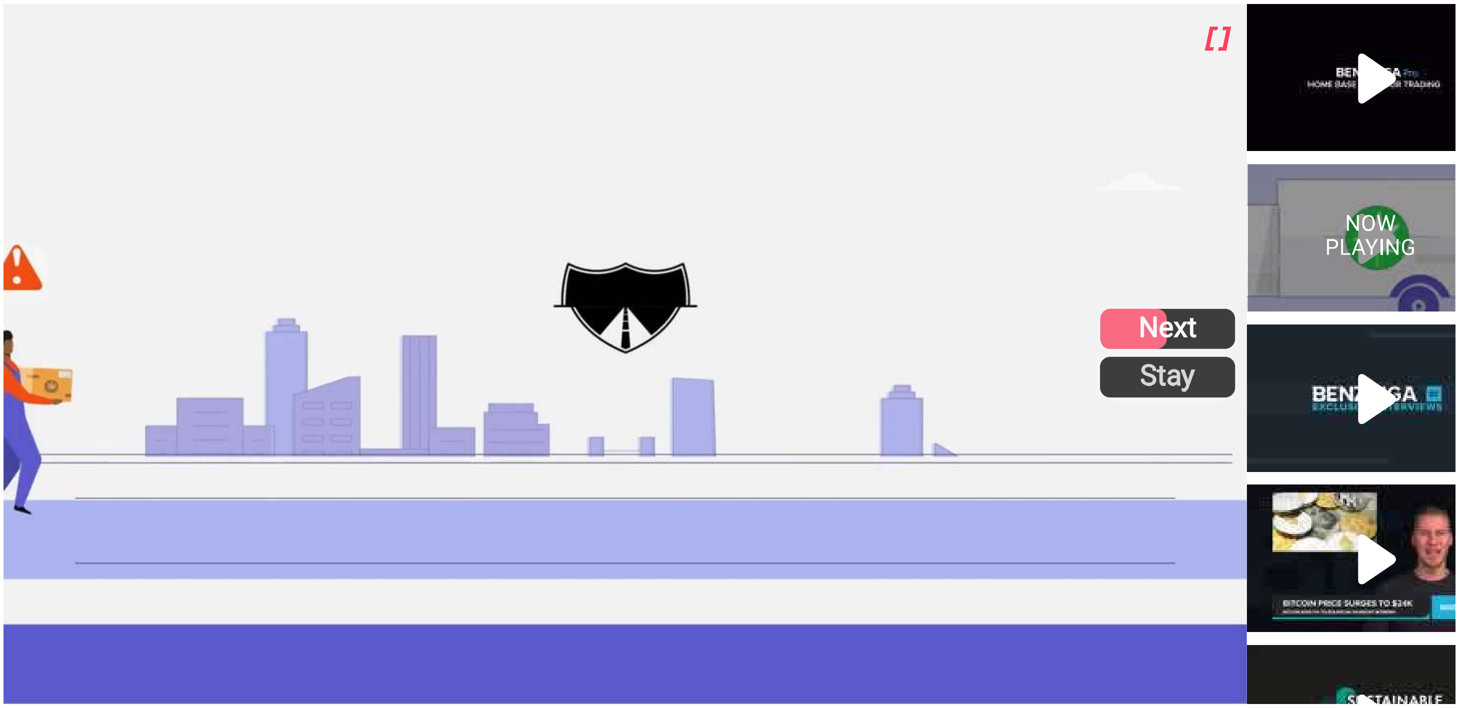
by Mehab Qureshi, Benzinga Staff Writer

January 3, 2023 4:55 AM | 3 min read

FOLLOW ON Google News

ZINGER KEY POINTS

- **Since its creation in 2018, the Lighting Network has seen immense adoption beyond its critics' expectations.**
- **The Lightning Network is totally decentralized and improves Bitcoin's scalability.**



Bitcoin ▲ BTC/USD +1.66% + Free Alerts experienced a tumultuous 2022, with price crashes and crypto collapses making headlines. Yet, this was also a year of immense progress for the world's largest cryptocurrency.

What Happened: The Bitcoin **Lightning Network**, a critical scaling protocol enabling near-instant, low-cost payments off-chain, underwent significant growth and evolution. We take a look at the Bitcoin Lightning Network and how it changed in 2022.

The Lightning Network is a revolutionary technology for Bitcoin (or satoshis, the smallest denomination of a Bitcoin) transactions. By increasing the capacity of the network, users benefit from faster payment speeds and larger transaction volumes, which come with lower fees.

Crypto is available to anyone wanting to get involved.
Cass,
Senior Product Specialist

Since its creation in 2018, the Lighting Network has seen immense adoption beyond its critics' expectations, with 4,000 BTC capacity in June and successful usage in locations such as **El Salvador**, the Isle of Man, and **Gibraltar**. Even Bitcoin influencer **Udi Wertheimer**, who had previously expressed doubts about the network's viability, has been forced to concede its “success”.

The Lightning Network is totally decentralized and improves Bitcoin's scalability. The publicly visible liquidity capacity rose from 1,058 Bitcoins to more than 4,771 Bitcoins in 2022. The number of Lightning Network channels increased by an impressive 80%, from 37,298 to 67,339 channels, as per 1ml.com lightning network tracker. Additionally, the number of public Lightning Network nodes rose by 88%, from 8,295 to 15,636 nodes (though the rate of growth slowed in the second half of the year).

and receiving of assets. Taro leverages the latest Bitcoin protocol upgrade, Taproot, to enable the issuance of practically any kind of asset on the Bitcoin blockchain that remains backed by the unchangeable security of Bitcoin's proof-of-work consensus mechanism. This opens the door for increased use cases and enhanced functionality on the network, such as the issuance of stablecoins, stocks and bonds on top of the Bitcoin protocol.

Impervious Technologies unveiled the world's first Web Browser powered by Bitcoin's Lightning Network. This Peer-to-Peer Browser offers a comprehensive set of communications, data transfer and payment tools without any centralized intermediaries. These include end-to-end encrypted messaging, video calls, collaboration platforms, decentralized identity management, data storage and giving users the opportunity to monetize their data.

Last but not least, **Value-4-Value**, an innovative approach to content publishing that rewards the creator with value after their customers enjoy the content. By leveraging the Lightning Network and utilizing solutions such as Lightning Addresses and Bolt-12 invoices, over 10,000 content creators have already implemented Value-4-Value on their podcasts.

Rene Pickhardt, Bitcoin Lightning Network developer, told **Benzinga** that the major breakthrough for the Lightning network was in March when he developed a new approach to massively improving lightning payments reliability.

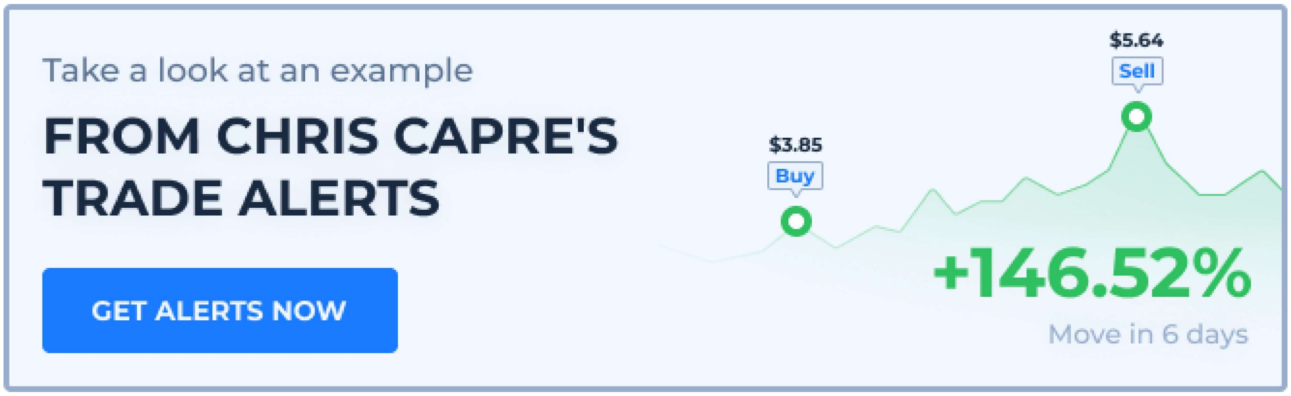
Pickhardt's research suggested that approaching the payment splitting process as an optimization problem can provide both reliability and cost-efficiency, leading to better outcomes.

The Future: A new report by Arcane Research titled "State of Lightning" says that the Bitcoin Lightning Network could have an astounding 700 million users by 2030.

According to this report, gaming and streaming video and audio will be major use cases for the Lightning Network, with streaming services like **Spotify** and **Netflix** digital payments industry — and change the way we consume media.

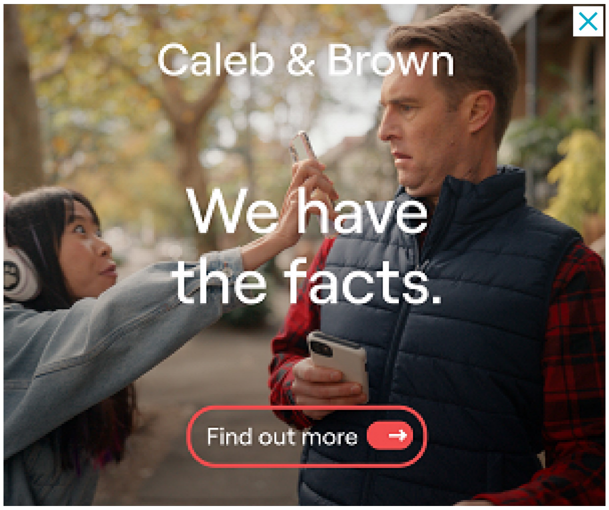
Price Action: At the time of writing, Bitcoin was trading at $16,842, up 0.02%, according to Benzinga Pro data.

Read Next: *Bitcoin, Ethereum Muted, Dogecoin Spikes: No Signs Of 'Santa Claus' Rally As Analyst Says Tech Rout Behind Risk-Off Mood*



© 2023 Benzinga.com. Benzinga does not provide investment advice. All rights reserved.

Posted In: El Salvador Lightning Network Rene Pickhardt Taro Cryptocurrency News Top Stories Markets Tech



BENZINGA Crypto

My Account

IN THE MARKETS: FEBRUARY 16, 2023

US Treasury Would Run Out Of Cash By This Time Unless Debt Ceiling Issue Resolved: Congressional Budget Office

Mystery Trader '50 Cent' Apparently Returns With Another Big Volatility Bet

This Expert Sees Gold Breaking $2,000 Level By End Of 2023 — Here's Why

Michael Burry, Farallon Capital, Coatue Management Bet Big On China Stocks In Q4

Bull And Bear Case For Trade Desk As The Stock Surges Higher

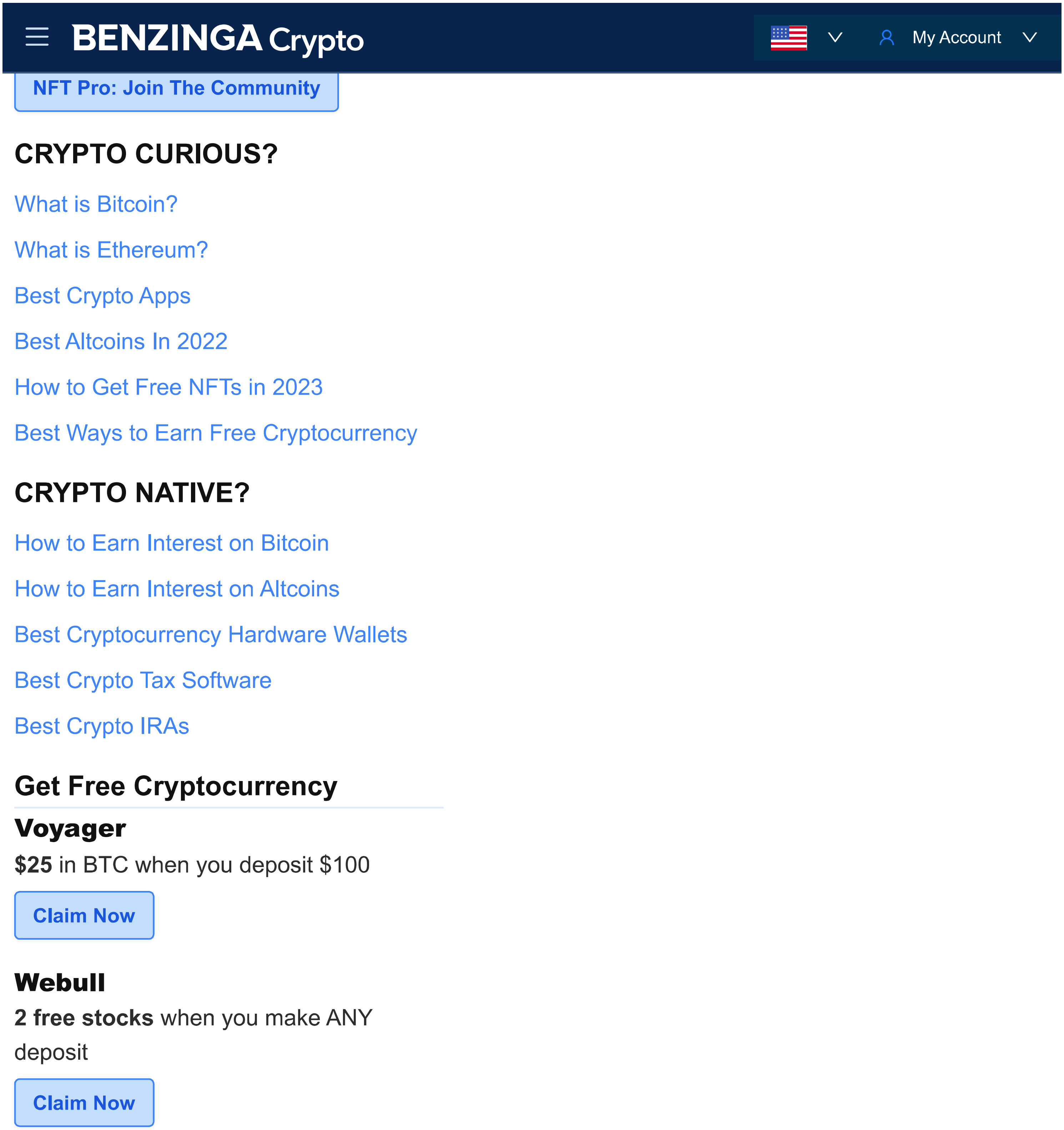
Inflation

Benzinga Crypto

1,000,000 monthly readers. Are you one of them?

Benzinga's Crypto News Hub

Benzinga's Crypto Education Hub



NFT Pro: Join The Community

CRYPTO CURIOUS?

What is Bitcoin?

What is Ethereum?

Best Crypto Apps

Best Altcoins In 2022

How to Get Free NFTs in 2023

Best Ways to Earn Free Cryptocurrency

CRYPTO NATIVE?

How to Earn Interest on Bitcoin

How to Earn Interest on Altcoins

Best Cryptocurrency Hardware Wallets

Best Crypto Tax Software

Best Crypto IRAs

Get Free Cryptocurrency

Voyager

$25 in BTC when you deposit $100

Claim Now

Webull

2 free stocks when you make ANY deposit

Claim Now

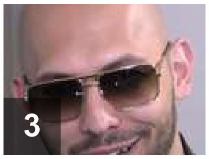
BENZINGA Crypto

My Account

Top Cryptocurrency News

1 Warren Buffett Now Owns Bitcoin: Here's How The Oracle Of Omaha Got Exposure

2 Shiba Inu Ecosystem Token Surges 9% After Lead Developer Says 'Shibarium Is Ready'


3 Kickboxing Star Andrew Tate, Brother Tristan Reportedly Say $467K Bitcoin Seized By…

4 Bitcoin Surges After Retracing To This Fibonacci Level: What's Happening?

5 Jordan Peterson Asks 3.8M Twitter Followers For Help In Joining Bitcoin Lightning Network

BENZINGA Crypto

My Account

Promise In Securing The Future Of Financial Cybersecurity

by Gita Karunakaran

February 15, 2023 8:06 AM | 4 min read

Advertiser Disclosure

Biometric systems are gaining immense popularity around the globe. They are easy to use and implement and provide a cost-effective solution for ensuring high-end cybersecurity.

Biometrics are unique physical characteristics, such as fingerprints or facial scans, that can be used for automated recognition. They're popular for being a reliable, secure, and practical means of identifying and authenticating individuals through their unique biological characteristics.

Over the years, biometrics has found widespread use in a variety of applications, including cybersecurity. Companies like **BIO-key International Inc.** ▲ BKYI +0.13% + Free Alerts, for example, use biometrics in their Identity and Access

Viable Financial Cybersecurity May Need More Than Traditional Biometrics In The Future

In most cybercrime cases, fraudulent activity is reportedly detected only after someone has already lost money or data to hackers. As such, any analysis commences only after the fact.

With cybercrime on the rise and financial losses from cybercrime projected to cost over $10.5 trillion annually by 2025, organizations are constantly on the lookout for fail-safe solutions to protect their brand and reputation from damaging breaches, proactively.

A branch of biometrics – known as behavioral biometrics – that has emerged from observing human behavioral patterns seems to hold promise in possibly pre-empting potential cybercrimes.

Behavioral biometrics track an individual's behavior patterns and the manner in which he or she interacts with the device itself, such as the way a screen is held, the manner of typing, and the speed at which the mouse is moved.

Biometric behavioral inputs, when collected and analyzed, can enable banks and financial services providers to flag potential fraud even before a transaction goes through. This enables them to take action to prevent it – either by halting the transaction or requiring additional authentication factors from the customer, before proceeding.

An additional benefit of behavioral biometrics is that the analysis can happen without extracting and storing data from the customer's phone or device, minimizing the chances of customer data being stolen or misused.

When It Comes To Reducing Fraud, Biometric Authentication Can Help Merchants

sufficient for merchants to successfully combat scams and hacks.

Equally, consumers are becoming more aware of cybersecurity risks and frauds, and have mounting concerns about safeguarding their payment information and other sensitive details while transacting online or even in person. As a result, customers are reportedly willing to take extra steps – including facial recognition – in authenticating their banking as well as non-bank accounts if it means a more secure experience.

However, there have also been concerns about the ability of facial recognition to prevent fraud when they are relied upon as the sole criteria to transact, especially if the face scan matches aren't verified through additional alternative means.

One of the solutions to this issue has been to adopt a hybrid fraud prevention tactic, which combines biometrics such as fingerprint identification or voice recognition with other identity authentication technologies. At the same time, privacy regulations continue to grow, putting pressure on organizations to adhere to multiple norms and regulations on the storage of biometrics.

All of this highlights the need to arrive at the right fraud-fighting tools to prevent revenue loss, customer asset loss, and brand reputation damage for organizations and merchants – to strike the perfect balance of data privacy and security.

The increased awareness of cybersecurity risks and a rise in the adoption of biometrics has also given rise to the growth of multi-factor authentication (MFA) – sometimes with more than one biometric method or multimodal biometrics as a preferred option for maximum protection against cybercrime, hacking, and fraud.

And increasingly, biometrics is seen as possibly the only security that can help banks, retailers and other organizations combat sophisticated fraud attacks, as fraudsters continue to use various tactics, including SIM swaps and porting scams, to redirect OTPs (one-time passwords) to a device they control or convince their victims to hand them over through deception or brute force attacks.

multi-factor options. The company believes that IBB is a way to establish trust and accountability. IBB enables organizations to confirm an individual's genuine presence when accessing systems and provides them with the ability to audit with full transparency.

BIO-key's single, unified IAM platform, PortalGuard, offers solutions for a range of use cases and business initiatives, such as MFA, Single Sign-on, and Self-service Password Reset.

PortalGuard requires only a one-time enrollment and can be quickly set up for access across multiple devices and locations according to BIO-key. This could offer greater deployment versatility and scalability and enable enterprises to provide a consistent and seamless user experience.

To learn more about BIO-key's identity-bound biometric solutions visit the company webpage here.

This post contains sponsored advertising content. This content is for informational purposes only and is not intended to be investing advice.

Featured Photo by Gerd Altmann from Pixabay

Posted In: BIO-Key Partner Content Small caps Penny Stocks Movers & Shakers General

Trending Articles

Tesla, Apple Stakes Slashed By Tennessee Treasury In Q4: Here Are Its Other Big Tech Holding Cuts

Bitcoin Target Of $42K 'More Conceivable' Now, Says Analyst Who Predicted May 2021 Crypto Crash

A pseudonymous crypto analyst who called May 2021 crypto crash said that $42,000 for Bitcoin (CRYPTO: BTC) "is more conceivable" as the apex crypto moves past $24,000.

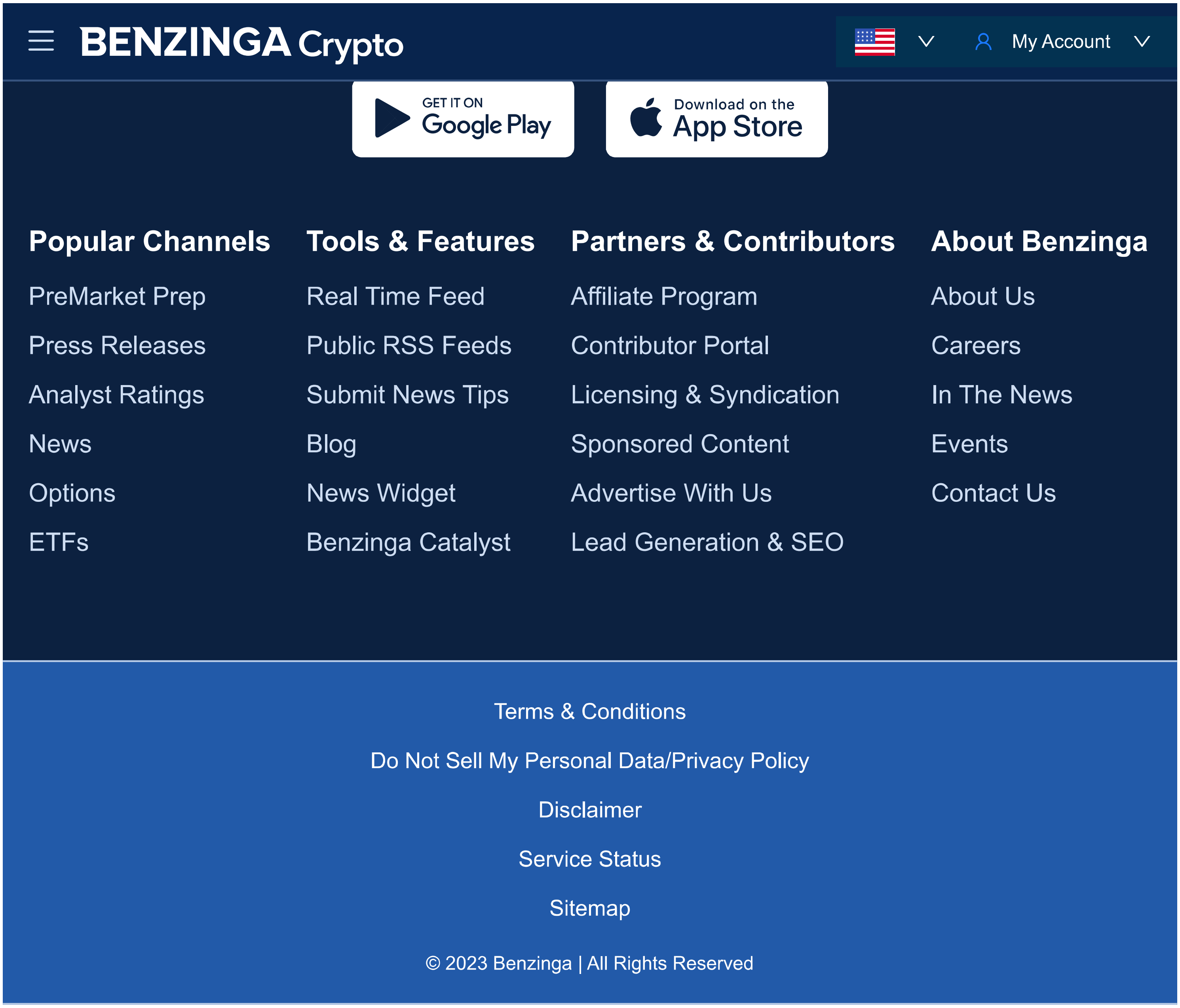
President Joe Biden said the U.S. and Canada acted together to take down at least three unidentified aerial objects in recent days. It is not yet known in which country the objects originated.

Paramount Adds 9.9M Streaming Subscribers In Q4: How It Stacks Up To Netflix, Disney+ And Other Rivals

The streaming market continues to be ultra-competitive, with streaming pure-play companies, media giants and others launching and growing their own platforms. Companies are looking for an edge with t…

Uh-Oh: Why These 2 Key Inflation Indicators Are Cause For Worry

A pair of economic indicators are injecting worry into market bulls Thursday morning. Here's a look at what the data means for the Federal Reserve, and ultimately the markets.



Popular Channels

PreMarket Prep

Press Releases

Analyst Ratings

News

Options

ETFs

Tools & Features

Real Time Feed

Public RSS Feeds

Submit News Tips

Blog

News Widget

Benzinga Catalyst

Partners & Contributors

Affiliate Program

Contributor Portal

Licensing & Syndication

Sponsored Content

Advertise With Us

Lead Generation & SEO

About Benzinga

About Us

Careers

In The News

Events

Contact Us

Terms & Conditions

Do Not Sell My Personal Data/Privacy Policy

Disclaimer

Service Status

Sitemap

LIGHTNING NETWORK

Taro Protocol Programmable Lightning Network Assets

Published 2 weeks ago on January 21, 2023
By **David Hamilton**

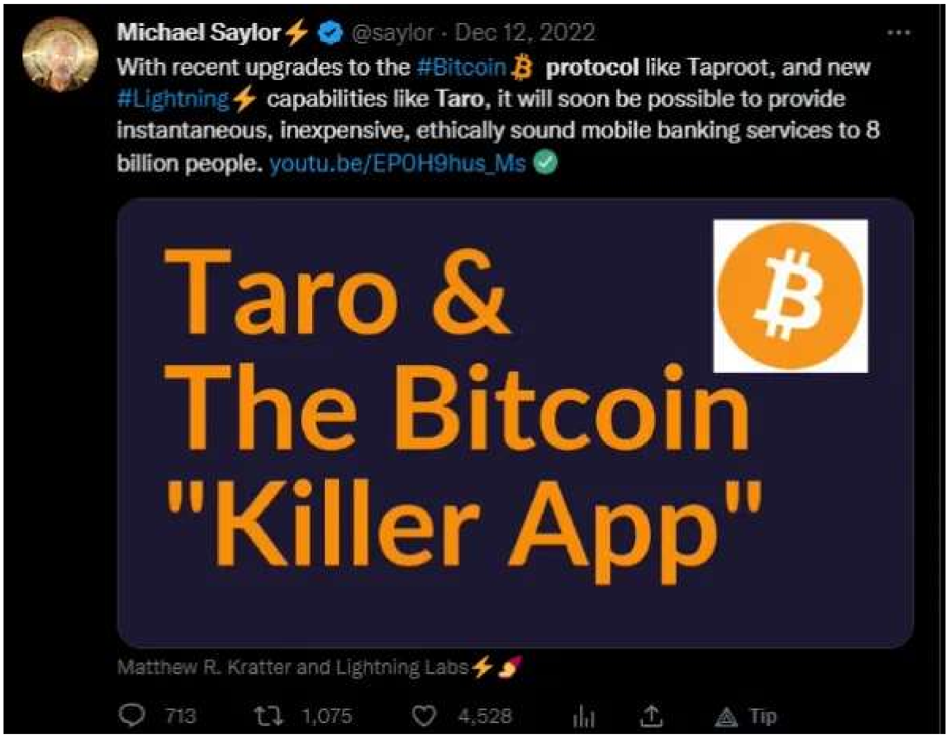
SEAR

The Taro protocol introduces a way for developers to integrate multiple assets across networks using the Lightning Network. The service makes it easy for designers to leverage the security of Bitcoin while reducing fees and transfer times. Here’s what makes the Taro protocol a game changer.

Transfer Stablecoins – Taro

The Taro system enables users to transfer stablecoins across networks using Bitcoin as the intermediary. The system leverages a new type of channel specially built for stablecoin transfers called an L-USD Channel. The channel ensures Bitcoin underpins all transactions which improves security and confidence in the system.

Bitcoin is the largest poW blockchain in the world and has operated successfully for 14 years. It has the most consumer confidence and enables developers to leverage these aspects of the project are sure to help drive interest.



Michael Saylor⚡ @saylor · Dec 12, 2022

With recent upgrades to the #Bitcoin ₿ **protocol** like Taproot, and new #Lightning⚡ capabilities like **Taro**, it will soon be possible to provide instantaneous, inexpensive, ethically sound mobile banking services to 8 billion people. youtu.be/EP0H9hus_Ms

Matthew R. Kratter and Lightning Labs⚡

Taro Protocol

The developers note that the system will improve remittance payments internationally. Remittance and other international money transfer methods are outdated. Taro provides another level of efficiency and traceability. Users can create digital assets with ease and all transactions get posted to the Bitcoin blockchain when the L-USD channel closes.

Fiat to Crypto On Ramp

The Taro protocol enables users to convert fiat into cryptocurrencies as well. This feature is a major plus as most people still use CEXs (centralized exchanges) to accomplish this task. Using a CEX is time-consuming, expensive, and requires a lot of personal information to be shared with a third party. As such, Taro provides a streamlined approach that will drive adoption.

Issuing Assets

The Taro system leverages the Taproot upgrade. The system uses a new data tree structure. This upgraded system supports more flexibility. For example, developers can embed arbitrary asset metadata within an existing output. The upgrade enables users to create stablecoins and other digital assets using Bitcoin. Taproot went live in November 2021.

The upgrade altered the way that scripts controlling coins are contained within a tree structure. The new setup supports private access to scripts. The main advantage is that developers can now create more complicated scripts. These scripts can be made at a lower cost than submitting data to the blockchain using the traditional keySpend path. Developers can use this service to attach verifiable data to transactions without revealing the data to other blockchain users as well.

High Performance

The system provides high performance and low fees to the community. Specifically, the technique integrates support for multi-hop transactions which cuts transaction processing time down. Additionally, the upgrade improves the network's audibility which will enable developers to create more complex assets like stablecoins that must remain regulatory compliant.

According to company documentation, the use of a Sparse-Merkle Tree enables the private retrieval of transaction data and validation services. Uniquely, the channel supports both Lightning Network transfers or directly sending assets on Bitcoin's mainnet.

Taro – Lighting Network Powered Stablecoins are on the Way

Protocols like Taro continue to demonstrate the resilience and overall flexibility of the Lightning Network. Developers are sure to leverage these tools to improve onboarding and support for stablecoins within their Dapps. As such, Taro is positioned to see growth in the coming months.

RELATED TOPICS: #STABLECOINS #TAPROOT #TARO

DON'T MISS

‹ Lighting Network Year in Review

YOU MAY LIKE

Lighting Network Year in Review

Lightning Labs Release Taproot Upgrade for the Lightning Network

Home About Us FAQ Press Tools Contact Us

Advertiser Disclosure: Bitcoinlightning.com is committed to rigorous editorial standards to provide our readers with accurate information. We may receive compensation when you click on links to products we reviewed.

Trading Risk Disclaimer: There is a very high degree of risk involved in trading digital assets. Trading in any type of financial product including digital assets, and cryptocurrencies involves a high level of risk.

This risk is higher with Cryptocurrencies due to markets being decentralized and non-regulated. You should be aware that you may lose a significant portion of your portfolio.

Bitcoinlightning.com is not a registered broker, analyst, or investment advisor.